ISTANBUL TECHNICAL UNIVERSITY ★ INFORMATICS INSTITUTE

SUBBAND DECOMPOSITION AND FRACTAL IMAGE COMPRESSION BASED STEGANOGRAPHY

M.Sc. THESIS

Suhad ALBASRAWI

Department of Applied Informatics

Applied Informatics Programme

DECEMBER 2017

ISTANBUL TECHNICAL UNIVERSITY ★ INFORMATICS INSTITUTE

SUBBAND DECOMPOSITION AND FRACTAL IMAGE COMPRESSION BASED STEGANOGRAPHY

M.Sc. THESIS

Suhad ALBASRAWI
(708151021)

Department of Applied Informatics

Applied Informatics Programme

Thesis Advisor: Assoc. Prof. Dr. Behçet Uğur TÖREYİN

DECEMBER 2017

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

ALTBANT AYRIŞTIRMA VE FRAKTAL İMGE SIKIŞTIRMA TABANLI STEGANOGRAFİ

YÜKSEK LİSANS TEZİ

Suhad ALBASRAWI
(708151021)

Bilişim Enstitüsü

Bilişim Uygulamaları Programı

Tez Danışmanı: Doç. Dr. Behçet Uğur TÖREYİN

ARALIK 2017

Suhad-ALBASRAWI, a M.Sc. student of ITU Graduate School of Informatics Institute student ID 708151021, successfully defended the thesis entitled "SUBBAND DECOMPOSITION AND FRACTAL IMAGE COMPRESSION BASED STEGANOGRAPHY," which she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor : **Assoc. Prof. Dr. Behçet Uğur TÖREYİN** ....
İstanbul Technical University

Jury Members : **Prof. Dr. Lütfiye DURAK ATA** ....
İstanbul Technical University

Assist. Prof. Dr. Ufuk ÖZKAYA ....
Süleyman Demirel University

Date of Submission : 17 November 2017
Date of Defense : 13 December 2017

FOREWORD

I would like to express my gratitude to Assoc. Prof. Dr. Behçet Uğur TÖREYİN - for his supervision, suggestions and encouragement throughout the development of this thesis.

I am also indebted to Prof Dr. Lütfiye DURAK ATA and Assist. Prof. Dr. Ufuk ÖZKAYA for accepting to read and review this thesis and for their suggestions.

It's a great pleasure to express my special thanks to my family who brought me to this stage with their endless patience and dedication. Finally, I would like to thank my friends, for their help during all stages of this thesis.

November 2017 Suhad ALBASRAWI

TABLE OF CONTENTS

ABBREVIATIONS

FIC	: Fractal Image Compression
DWT	: Discrete Wavelet Transform
Ic	: Cover Image
Is	: Secret Image
E	: Entropy
PSNR	: Peaks Signal-to-Noise Ratio
MSE	: Mean Squared Error
STFT	: Short Time Fourier Transform
CWT	: Continuous Wavelet Transform
FFT	: Fast Fourier Transform
Db1	: Daubechies one (Haar wavelet filter)
CR	: Compression Ratio
DES	: Data Encryption Standard
LSB	: Least Significant Bit
1D	: One Dimension
2D	: Two Dimension
1-level	: One Level
PSNR	: Peaks Signal-to-Noise Ratio
FWT	: Forward Discrete Wavelet Transform
SSIM	: Structural Similarity index
COR	: Correlation
BSM	: Binary Similarity Measure

SYMBOLS

$\psi(t)$	: The Haar wavelet's mother wavelet function
$\phi(t)$	: Scaling function
t	: Time
α_{ij}	: The pixel of the cover image in the (i, j) coordinate
β_{ij}	: The Pixel of the stego image in the (i, j) coordinate
(m, n)	: The size of the cover image and stego image
r	: Row number
c	: Column number
m	: Height of the cover-image
n	: Width of the cover-image
$c\ (r, c)$	: Cover-image
$\bar{c}$	: Mean square error of cover
$\bar{s}$	: Mean square error of secrte
$H(C)$	: The entropy of cover image
$H(S)$	: The entropy of secret image
$p(x_i)$	: Includes the histogram counts returned from image histogram
Ku	: The coefficient
σx^2	: The variance of x
σy^2	: The variance of y
$Cov(x,y)$	: The covariance of x and y
μx	: The mean values of x
μy	: The mean values of y
u, i	: (1,2,3, …, N)
N	: The number of coefficients
α	: The Alpha factor
K	: Dimension of block size
T	: Threshold
σ	: Standard Deviation
x_i	: The coefficient value

LIST OF TABLES

Page

LIST OF FIGURES

Page

SUBBAND DECOMPOSITION AND FRACTAL IMAGE COMPRESSION BASED STEGANOGRAPHY

SUMMARY

This thesis proposes a novel steganographic algorithm for embedding secret image data into digital cover images. The proposed method consists of two stages. The first phase is the embedding. We start by calculating the entropy for cover image and secret image to assess the amount of information that is not compressible. We use discrete wavelet transform for cover image, and via a certain threshold value many coefficients are set to zero. We used the threshold in the wavelet domain to identify insignificant coefficients, so thresholding will be used as a method to determine the hiding map. We use Fractal Image Compression (FIC) for secret image which yields the outcome as a group of affine transformations, and then take Huffman code the result.

After compressing the secret image information with Huffman code, it's necessary to store the data in a special way, because the output of the encoder is a stream of 1's and 0's, hence the stream must be converted into 8-bit-long chunks and stored. In addition, the code dictionary which is needed for the decoding process, must also be stored. Again, the dictionary is a group of 1's and 0's changing in length depending on the code generated, which, in turn, is a representation of the probability of the data symbols in the secret image as affine transformations.

In the embedding stage, a secret vector is synthesized from the secret image. In other words, the group of information that is output from secret image makes up the so called "secret vector". A necessary piece of information is the length of the stream and whether it is divisible by 8. If so, another byte (8 bit) is added to the secret vector. The secret vector contains the binary stream which specifies the number of zero bits added to complete the stream to make the length of the code a multiple of 8. If there is no remainder, this byte contains the zero value. The byte is added after encoded data and the dictionary. Then secret vector is rescaled to get the highest PSNR for the cover image versus the stego image.

The second phase is the extraction. The cover image is decomposed by using wavelet transform. Threshold value is calculated for the wavelet coefficients. Then a search for insignificant coefficients (less than threshold value) is initiated. The same threshold value should be guaranteed to find the same locations where we stored our secret vector. When the secret vector is found, it is rescaled back to its normal value by dividing it with the threshold value then multiply it with maximum value which is followed by Huffman decoding. Then just after this step, the fractal image iterations are carried out to rebuild the secret image as close as possible to the original image.

The proposed algorithm of steganography to embedding secret image in cover image was tested over different cover images and secret images. The scheme performs well in terms of compression ratio, resolution and security. The threshold value was used as a method to determine the hiding map and to extraction. And by using the thres-

hold value, the process becomes more secure. PSNR values for Cover image and Stego image for different secret images were ranging from 39 to 62, and the correlation was ranging from 0.995914 to 1.0000. The compression ratio was ranging between 29% to 35.6%. Results of extracted images were of high quality. Disadvantages associated with this method is that the time, due to a lot of from processing be made to obtain high quality. Results demonstrate its effectiveness, robustness and security.

ALTBANT AYRIŞTIRMA VE FRAKTAL İMGE SIKIŞTIRMA TABANLI STEGANOGRAFİ

ÖZET

Steganografi veri güvenliğini sağlamak için kullanılan bir teknik olup Yunanca kökenli bir kelimedir ve iki kelimeden oluşur: çatı veya kapatılmış anlamına gelen stegos ve yazmak anlamına gelen grafik. Bu teknik, gerçekleşen iletişimin asıl içeriğini saklama sanatı ve bilimidir. Steganografi kullanımı sayesinde, şüphe uyandırmayacak bir bilgi içerisine gizli bir mesaj yerleştirmek ve bunu kimsenin varlığından haberdar olmayacağı bir biçimde göndermek imkanını sağlar. Steganografi, içerisine yerleştirildiği veride büyük bir değişiklik yapmadan dışarı alınamayan gizli haberleşme yöntemleri sağlar. Saldırgan tespit edecek bir yöntem bulamadığı sürece yerleştirilen bilgi gizli kalacaktır.

Birçok insan kişisel, tıbbi veya başka nedenlerden dolayı görüntü değişimi yapmak istemekte ancak başka kişiler tarafından (üçüncü taraflar) görülmek istememektedir, çünkü bu durum mahremiyetin ihlalidir. Bu nedenle, hem kayıt esnasında hem de gönderimi yaparken güvenlik gerekmektedir. Bu sorunu çözmek adına mevcut tez içerisinde, gizli görüntü verilerinin dijital kapak resimleri içerisine yerleştirilmesi için modern bir steganografik algoritma tanıtılmaktadır. Önerilen yöntem iki aşamadan oluşmaktadır.

Birinci aşama yerleştirme aşamasıdır. Öncelikle sıkıştırılamayacak bilginin miktarını öğrenebilmek adına kapak resmi ve gizli resmin entropisini hesaplayarak başlıyoruz. Kapak resmi için gizli bir dalgacık dönüşümü kullanıyoruz, ve belli bir eşik değer üzerinden birçok katsayı sıfıra ayarlanıyor (dalgacık dönüşümündeki eşiği gereksiz katsayıların belirlenmesi için kullandık ve bu nedenle eşikleme yöntemi gizli haritanın belirlenmesi için bir yöntem olarak kullanılacak). Gizli resim için Fractal Image Compression -FIC (Oransal Görüntü Sıkıştırma) yöntemi kullanıyoruz. Ortaya çıkan sonuç bir grup afin dönüşüm olacaktır. Sonrasında bu sonucun Huffman kodunu alıyoruz. Gizli resmi Huffman kodu ile sıkıştırdıktan sonra veriyi özel bir şekilde saklamak önemlidir çünkü kodlayıcının çıkışı bir dizi 1 ve 0'dır ve bu nedenle bu serinin 8 bit gruplara dönüştürülmesi ve hafıza kısmına normal bir biçimde 8 bit ikili numara olarak saklanması gerekir. Ayrıca, kodu çözme işlemi için gerekli olan kod sözlüğünün de kayıt edilmesi gerekmektedir. Yine sözlük, oluşturulan koda bağlı olarak farklı uzunluklara sahip 1 ve 0 gruplarından meydana gelmektedir ve bu kodlar, gizli resim afin dönüşümündeki veri sembollerinin olasılığının bir temsilidir.

Yerleştirme aşamasında, gizli resimden bir gizli vektör sentezlenir, bir başka deyişle gizli resmin çıkışı olan bilgi grubu "gizli vektör" adını verdiğimiz oluşumu meydana getirir. Gerekli olan bilgilerden bir tanesi stream serisinin uzunluğu ve 8 ile bölünüp bölünmediğidir. Eğer bölünüyorsa, gizli vektöre başka bir bayt (8 bit) eklenir. Gizli vektör içerisinde yer alan ikili stream, stream'in hiç kalan olmadan 8 ile bölünebilmesini sağlamak için eklenmesi gereken sıfır bit miktarını belirtmektedir.

Eğer kalan yoksa, bu bayt sıfır değerini içermektedir. Baytın eklenmesi kodlanmış veri ve sözlükten sonradır.

Sonrasında gizli vektör yeniden ölçeklendirilir (kapak resmi için stego resme karşı en yüksek PSNR'i elde etmek için, bir başka deyişle stego resmin kapak resme benzer olabilmesi için tüm gizli vektörü maksimum değerine bölüp eşik değeri ile çarpıyoruz, maksimum değer dalgacığın eşik değerine eşit veya daha düşüktür, bu nedenle dalgacık tersine çevrildiğinde kapak resmi ya hiç değişmeyecek ya da çok az değişecektir) ve sonrasında da sıfırlanmış dalgacık katsayıları içerisine yerleştirilir. Yeniden ölçeklendirme işlemi eşik değerini geçmemelidir, ki bu sayede sonradan hesaplabilir.

İkinci aşama çıkarma işlemidir. Dalgacık dönüşüm yolu ile kapak resmi ayrıştırılır. Dalgacık katsayıları için eşik değeri hesaplanır. Sonrasında (eşik değerinin altında olan) önemsiz katsayılar için arama başlatılır. Gizli vektörümüzü sakladığımız konumları bulabilmemiz için aynı eşik değerin bulunması gerekmektedir (gizli vektörü çıkartmak için eşiklemeyi kullanıp gizli haritayı belirlemek). Gizli vektör bulunduğunda normal değerine tekrar ölçeklendirmek için önce eşik değerine bölünür sonrasında da dalgacığın en yüksek konumunda saklanan maksimum değeri ile çarpılır ve bu sayede değer tüm aralık boyunca yayılır ve vektör analizi başlatılır. Bu analizle birlikte Huffman kodu çıkarılır ve ilk şekli olan bir ikili stream şeklinde tutulur. Sonrasında sözlük çıkarılır. Sözlük de aynı şekilde, her grubun kodlandığı sembole karşılık gelen bir hücrede tutulduğu bir dizi ikili bitten oluşur. Bunun anlamı şudur ki, ilk ikili model sıfır sembolünün kodudur. Bir Huffman kod çözme işlemi gerçekleştirilmiştir. Bu işlemin hemen ardından gizli resmi gerçek resme mümkün olduğunca benzer şekilde tekrar oluşturabilmek adına fraktal resim yineleme işlemi gerçekleştirilir.

Gizli resmin kapak resme yerleştirilmesi için önerilen steganografi algoritması çok farklı kapak resimleri ve gizli resimler üzerinde denenmiştir. Yüksek sıkıştırma oranı, yüksek çözünürlük, yüksek güvenlik ver resmi saklama kapasitesi anlamında bu işlem oldukça iyidir. Eşik değeri, gizleme haritasını belirlemek ve çıkartma işlemi için bir yöntem olarak kullanılmıştır. Ve ayrıca eşik değeri kullanıldığında işlem çok daha güvenilir hale gelmektedir. Sıkıştırma ve entropi arasında tersine bir ilişki vardır, bir başka deyişle dijital resmin entropi ölçüsü azaldıkça sıkıştırma oranı artmaktadır. Test edilmiş olan farklı gizli resimlerin Kapak resmi ve Stego resminin PSNR'si 39 ila 62 arasında değişmiş olup korelasyon 0.995914 ila 1.0000 arasında gerçekleşmiş ve sıkıştırma oranı da %29 ila %356 arasında değişmiştir. Çıkarılan resmilerin kalitesi yüksek olmuştur. Çıplak gözle bakıldığında kapak ve stego resmi arasında fark ayırt edilemez düzeydedir.

Bu yöntemin dezavanatajları arasında ise zaman bulunmaktadır. Çünkü yüksek kaliteye sahip bir sonuç elde edebilmek için çok sayıda işlem yapmak gerekmektedir. Tekrar boyutlandırma, rotasyon ver flipping gibi manipülasyon saldırılarına karşı yapılan steganografi testleri flip ve rotasyon ile bunların kombinasyonları saldırılarına karşı dayanıklılık olduğunu göstermiştir. Ancak yeniden boyutlandırma saldırısı testi başarısız olmuştur. Genel olarak elde edilen sonuçlar mahremiyeti korumak adına bu yöntemin etkin, güçlü ve güvenli olduğunu göstermektedir. fractal ve Huffman yöntemlerinin beraber kullanımı sıkıştırma oranını daha da arttırır. Gizli vektörü mümkün olduğunca küçük boyutta tutabilmek adına steganografi yüksek sıkıştırma oranı gerektirir.

Dalgacık kullanarak ayrıştırma yaptıktan sonra bir dijital resmin yüksek frekanslı parçaları içerisinde gizli bilgilerin depolanması, bu bilgilerin insan gözü ile görülebilmesini çok zorlaştırır. Bu tür bir tekniğin kullanımı sayesinde çok sayıda önemsiz katsayı elde edilir. Bu önemsiz katsayılar, görünen resmi çok bozmadan mümkün olduğunca çok miktarda gizli bilginin yerleştirilmesini sağlar. Yerleştirme işlemi esnasında hesaplanan belirli bir eşik değerinin kullanılması bir resmin içerisindeki gizli bilgilerin çıkartılmasını daha zor hale getirir. Eşik değeri, ortalama katsayı değeri kullanımından daha fazla konum oluşturmada etkinliği gözlemlenmiş olan katsayı değerinin standart sapması ile hesaplanır. Başka bir resim aynı haritayı oluşturamaz. Harita, kapak resmine bağlı olarak bir yandadır, gizli resme bağlı olarak da diğer yandadır. Daha fazla güvenliği sağlayacak doğru haritalamayı belirlemek kolay değildir.

Quad tree (Dördün Ağaç), kodlama yaparak dönüştürmek, bir eşik değer bulmak ve bunu gizlemek gizli bilgiyi doğru çıkartmayı, hata tamamen yok etmeden çıkartmayı çok zorlaştırır. İki kez dönüştürülmüş olan (fraktal ve Huffman ile) gizli bilgiye göre harita oluşturmak, gizli bilginin tespit edilmesi ve çıkartılmasını çok zorlaştırır.

Damgalama (watermarking) ve steganografi hedefleri arasında tercih yaparken her zaman için ödün verilecektir. Bir denge üçgeninde kapasite, güvenlik ve sağlamlık üç hedeftir, ve bu üç hedeften herhangi ikisini maksimize ederken diğer hedef minimize olur. Bir başka deyişle, Steganografi algoritmaları genellikle bilgi mesajını çıkarırken veya modifiye ederken yüksek güvenlik sağlamak zorunda kalmazken, Watermarking yöntemleri ise gizli mesajı çıkarırken veya modifiye ederken çok sağlam olmak zorundadır. Bizim algoritmamızda, yüksek güvenlikli olan bilgiyi saklarken kapasite ve kabul edilebilir sağlamlık arasında bir denge kurduk.

Genel olarak, saldırılara karşı direnç gösterilip tersine çevrilebilir ve bu nedenle stego korunarak çıkartma işlemi başarıya ulaşır. Bu durum tespit ve geometrik saldırılar (rotasyon, flipping vs.) yolu ile kendini gösterirken görüntü işleme saldırıları da ciddi bir başarı oranı göstermektedir. Gamma. Tersine filtre kullanmak sureti ile tersine çevrilebildiği için bileme (sharpening) saldırısı da çok yüksek bir başarı oranına sahiptir. Görüntünün renklerinde beklenmedik değişimler olup dalgacık dönüşümü etkilendiğinde yapılan saldırı ve bıraktığı etkilerin farkına varılabilir. Dalgacık dönüşümü olduğunda gizli vektörün konumu bulunamaz ve gizli mesajı çıkartmak imkansız hale gelir. Resme ses de eklenebilir. Bunun için görüntüye bir spot eklenir ve bunun boyutu değiştirilir. Bu spotun boyu çok fazla büyük olsa bile başarı oranı yüksek olur. Spot eklemek görüntüyü etkiler ve boyutu büyüdükçe PSNR oranı düşer ancak buna rağmen gizli mesaj çıkartılabilir.

1. INTRODUCTION

Widespread utilization of wireless data communication equipment, coupled with the availability of higher bandwidths, has driven to boosted user request for content-rich media like images and videos. In general people want to keep the contents of their communications private. Information hiding is a general encompassing many sub-disciplines, there are two important types namely steganography and watermarking [1, 2]. Steganography services to hide secret messages in other messages. Generally, the sender writes an innocuous message and then conceals a secret message in the same piece of paper. Hiding message with steganography reduces the chance of message is detected [3, 4].

Some organizations strive to avoid enemy's detection when the secret message is transmitted such as military and intelligence agencies etc. [5]. Also, both digital election and digital cache also require anonymous communication techniques such as protecting his identification and benefit for avoiding being misappropriated [6]. As audio, video and other works become available in digital form, the ease with which perfect copies can be made, may lead to large-scale authorized copying, which might undermine the music, film book and software publishing industries [7]. It is also used in medical clinics to hide medical images from manipulators and attackers to provide secure medical image transaction as the exchange of medical reference data [8].

These interest over protecting copyright have triggered important research to find ways to hide copyright message and serial numbers into digital media; the idea is that the letter can help to identify copyright violators, and the former to prosecute them. At the same time, moves by different governments to limit the availability of encryption services have encouraged people to study methods by which private messages can be embedded in seemingly innocuous cover message. Another reason to use information hiding is that some countries do not permit using cryptography, therefore, information hiding becomes the means by which people can hide their encrypted message [1,8].

1.1 Steganography

Steganography is a technique used to ensure the security of data, coming from the Greek two words: stegos, meaning roof or covered and graphic which means writing, is the art and science of hiding the reality of communication are taking place. The using of steganography gives the possibility to embed a secret message inside a piece of unsuspicious information and send it without anybody know of the presence of the secret message.

Steganography and cryptography are closely related. Cryptography scrambles secret messages thus it cannot be understood. Steganography otherwise, will hide the message so there is no knowledge of the presence of the message in the first place. In some cases, sending an encrypted message will trigger suspicion whereas an" invisible" message will not do so. Both sciences can be combined to make best protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques [9].

Steganography and encryption are both utilized to ensure data confidentiality. but, the major difference between them is that with encryption any person can see that both parties are communicating in secret. Steganography hides the presence of a secret message and in the best situation nobody can see that both parties are communicating in secret. This makes steganography suitable for some a task for which encryption isn't, such as copyright marking. Supplement encrypted copyright information to a file might be easy to remove but embedding it within the contents of the file itself can prevent it being easily identified and removed [10].

Steganography supply a means of secret communication which cannot be removed without important changing the data in which it is embedded. The embedded information will be confidential unless an attacker can find a way to detect it [11].

1.2 Terminology

There are four important terms in steganography:

1. Cover Image: The container in which we will put the secret image in.
2. Secret Message: The message that we want to embed in the cover image.
3. Stego Image: The resulting image after embedding the secret message in the cover image.
4. Extracted image: Secret message after extracting it from Stego image.

1.3 History

Usage of steganography method dates back to the ancient Greek times, when there were tattooed messages on people's shaved heads and then let their hair grow thus the letter remained unseen. A different technique at that time used wax tables as a cover source. Text was written on the underlying wood and the message was covered with a another layer from wax.

In the 20th century, secret inks were a great used technique. In the Second World War, the nation used milk, vinegar, fruit juices to write secret messages. When heated, these fluids be darker and the message could be read. Even later, the Germans progressing a method namely the microdot. Microdots are photographs with the size of a printed period however have the clarity of a standard typewritten page. The microdots were then printed in a letter or on an envelope and being very small, they could be sent unnoticed. Recently,

Steganographic methods have been used with success for centuries already. but, since secret data usually has a value to the ones who are not allowed to know it, there will be people or organizations who will try to decode encrypted data or find information that is hidden from them. Governments want to know what civilians or other governments are doing, companies want to be sure that trade secrets will not be sold to competitors.

Plentiful different motives are present to detect the use of steganography, so methods to do so continue to be developed whereas the hiding algorithms become more advanced [12,13].

1.4 Problem Definition

As a result of globalization trend, all transactions shall be in electronic form and is treated by any computer it is a technique which dominated the entire world because of these developments and increasing the transactions to be secure data increase the proportion of the problems faced data, such as interference or manipulation of data and these problems may lead disasters.

To further secure the data will be stored inside image as a cover for secret data (data to be sent), to work on securing confidential data better. We will use one of the techniques of steganography.

After applied fractal image compression and Huffman encoding for the secret message is embedded in the cover image after processing by wavelet transforms, in order to support the process of concealment to accomplish the highest security so as to not get to confidential data with ease.

1.5 Motivation

The major focus is to provide secure transmission of images, as the exchange of data achieved by not safe open networks leads to the case of alters to happen in secret images and creates the undesirable results. Therefore, we tried to find a method to hide secret images to send and receive them in a safe manner and with minimal noise [14].

1.6 Contribution

Steganography depends primarily on the amount of redundant data contained inside an image. Information can be embedded inside the "insignificant" and "un important "information inside a cover image (this depend on the threshold value condition). In a cover image we seek redundant data to use it as a vessel, and in a secret image we use redundant data to shorten amount of data needed to be hidden inside a cover image. using wavelet to embed information produces a large amount of hiding places inside an image this information can be retained successfully while manipulating in the unseen frequencies inside the cover image. A new concept of detecting places where the secret is hidden (map) is used depending on a values(secret information) that is hidden in a known location then a scan is made to compare which coefficient is satisfying the threshold value condition. Each location satisfy the condition is considered part of the map and the content is part of the hidden information. Then an extraction procedure is commenced. This new concept makes no significant addition to the image and uses no other massive changes in the image to store when the secret image is hidden. The threshold value not only can be transmitted but also can be calculated opening the possibility that nothing is sent separately to the receiver other than calculating from the same image.

1.7 Aim of the Thesis

The aim of this work added it the security of secret data by using steganography.

1.8 Organization of the Thesis

This thesis is organized into five chapters and the summary of their contents is given below:

Chapter two: Theoretical of Steganography and techniques used in the hiding, how to applying Steganography in multimedia (image, Audio, video) detection of steganography, and concept for wavelet transforms and fractal image decomposition.

Chapter three: The proposed method for steganography.

Chapter four: Gives the evaluation of tests and results.

Chapter five: Includes the conclusions and the recommendations for future work.

2. RELATED WORK

2.1 Introduction

Due to the importance of steganography to protect secret data from any exposures out sourcing in this chapter talked about the steganography in detail ,and how to apply the steganography and techniques of steganography that characterizes this science and detecting & defeating of steganography and relationship of watermarking with steganography. As well as some important concepts used in our algorithm.

2.2 Literature Review

Many studies and ideas have been used in the recent years in steganography where hiding information is a method to disguise secret information in an innocent image while the methods are different in many ways but there are certain qualities to focus on where the cover image redundant information and compressibility of the secret image allows a space to hide information. Also there are certain limitations like the size of the secret image and what size of a cover image can be used and what kind of measurement is necessary to find the limits. The Table 2.1 shows a number of previous researches summary, where those methods are surveyed and a plan to use and propose a new method from them.

Chin-Chen Chang et al. [15], described a method for hiding a secret image within a cover image by using the fractal image compression approach for secret image, and then encrypted using DES. finally embedding the encrypted data into the middle frequency DCT for the cover image. The method to determine the efficiency of embedding is the measurement of MSE and PSNR. The study claims the ability of storing large images inside smaller cover images though the study considered hiding 256×256 and 512×512 inside a cover of 512×512. The prime idea to be considered here the use of fractal image decomposition to achieve high compression rate although there is no mention of the compression ratio gained in this study. Although the outcome is obvious since the extracted affine transformations give a small amount of information when compared to the original image.

Al-Ataby and Al-Naima, [16] start by determination of a cover image’s redundant bits, and secret key to encrypt the hidden message that will be encapsulated inside a cover media. They used cryptography as a method to secure the secret image, symmetric encryption was followed.Converting cover image to discrete Wavelet transform, and then calculate the threshold that will identify a cover image’s redundant bits that can be used to embed the message. Convert the secret image to 1D bit stream encrypted bit stream of the message, then take DWT transform of the encrypted message. Finally, put the DWT coefficients of the encrypted message in the location specified previously in the DWT of the cover message. Inverse DWT transform to the result. This method allows high payload (capacity) in the cover image with very little effect on the statistical nature of it, the robustness of the steganography method will be enhanced. The drawback of the proposed method is the complexity and computational overhead, and if anyone gets the secret key, he or she can use it to decrypt all the information that was encrypted with the key. The largest payload being 73% of the cover size.

Table 2.1 : Previous researches summary.

Date	Research Title	Secret Processing	Hiding Technique	Security	Compression Ratio and Capacity	Secret Size
Jun-05	ADCT-domain System for Hiding Fractal Compressed Images	Fractal Compression	DCT middle frequency	Encryption of secret data	High CR not mentioned	512 square
Oct-10	A Modified High Capacity Image Steganography Technique Based on Wavelet Transform	Encrypted bit stream	Wavelet based upon thresholding	use of a DES encryption	73.83% largest possible load	no mention
Jun-12	Image Steganography Scheme using Chaos and Fractals with the Wavelet Transform	Wavelet Transform	Logistic Map for Wavelet transform	Complexity of the wavelet function used	no compression	256×256 largest
Mar-13	Multi Secure and Robustness for Medical Image Based Steganography Scheme	Wavelet Transform and mixed with dummy image	Wavelet transform and fused with secret	Container image must be at both receiver and transmitter for extraction	no compression	no mention
Feb-14	Steganography Using Fractal Images Technique	bit stream	Fractal block decimation hiding using least bit	Least bit in a fractal Pif's hard to notice and hard to guess	no compression	165×192
Jun-16	Image Steganography using Block Level Entropy Thresholding Technique	Message replacing	Block Entropy of DCT middle frequency	security by the complexity	no compression	no mention
Oct-17	A modified DWT-based image steganography technique	Wavelet Transform	Wavelet based upon thresholding	secret key computation	no compression	256×256

Yue Wu and Joseph P. Noonan, [17] described an embedding the secret image in the cover image The point of interest in this study is the use of wavelet identifying redundant information which they can be used to hide information without a visible change in the cover image. The method to determine the efficiency of embedding is the measurement of MSE, PSNR vs capacity. The proposed method uses a fractal image decomposition as the cover image. Moreover, the wavelets used to transform the cover image and the secret message. The wavelet transform ensures the secret image is only embedded within edges with the least visible human eyes. They directly used the wavelet coefficients to embed the message, results demonstrate its effectiveness and robustness. This paper also uses RMSE and PSNR to determine efficiency of embedding. While a try for different wavelets are tested against many filters to determine wavelet efficiency.

G. Prabakaran, R. Bhavani ,and P. S. Rajeswari, [18] they proposed a method uses integer wavelet transform (IWT) to safeguard the MRI medical image of a patient into a single container image. Firstly, the dummy container image was produced .by applying flip left for the container image. And Arnold transform was applied for secret image (medical image), the result that is obtained scrambled secret image. Secondly, embedding the scrambled secret image into the dummy container image, and then taking Inverse IWT to get a dummy secret image. Thirdly, fuse container image with dummy secret image the output is stego image. The quality of the recovered medical image appeared acceptable visual quality. The method uses entropy of small blocks to encode the secret image over the cover image. The measurement is also used RMSE and PSNR to determine the efficiency of embedding. The entropy of blocks shows almost similarity for small blocks.

Prof. Dr. Tawfiq Abdulkhaleq Abbas, Hassanein Karim Hamza, [19] described a method where the cover image is divided into small image(blocks), then fractal is taken to each block. The size of blocks must not be less than 32 then quad tree decomposition is applied which is the range of the fractal and the domain is formed by the subset of subband. Using PIFS algorithm fractal affine is composed by finding similarities between range and domain, and then select the regions that will be used to hide the secret. There is a balance between the quality of the produced image and the amount of data. This paper uses RMSE and PSNR vs different sizes to evaluate the efficiency. Also, it opens the way to the idea of using another fractal technique to compress the image.

S. Pal Samir Kumar Bandyopadhyay, [20] proposed a method of steganography based on entropy level comparison in the DCT converted cover blocks of size 8×8 allowing the secret to being hidden inside the blocks with the highest entropy this method allows a changing map according to the entropy, hence according to the cover image. The prime idea here is to embed the changing map according to the cover image which gives us an idea to use such a technique in hiding our keys to extracting the secret. The use of information embedded according to the cover is very important not to have a shared key between receiver and transmitter for each secret.

Vijay Kumar and Dinesh Kumar [21] proposed a method of steganography based on Discrete Wavelet Transform (DWT), they proposed to reduce deformation in the cover image based on two concepts. The first concept makes the calculation of the secret key more powerful. The second one ensures that the difference with the original cover image is minimum.

2.3 Steganography

Steganography is the ability to hide information within a particular source of data that appears to be above suspicion to the naked eye. In other words, steganography is the ability to hide information from plain sight.

Using steganography enforces embedding secret information inside a piece of unsuspicious information and sends it without anyone knowing the existence of the secret message [22]. Figure2.1 shows the process of steganography.

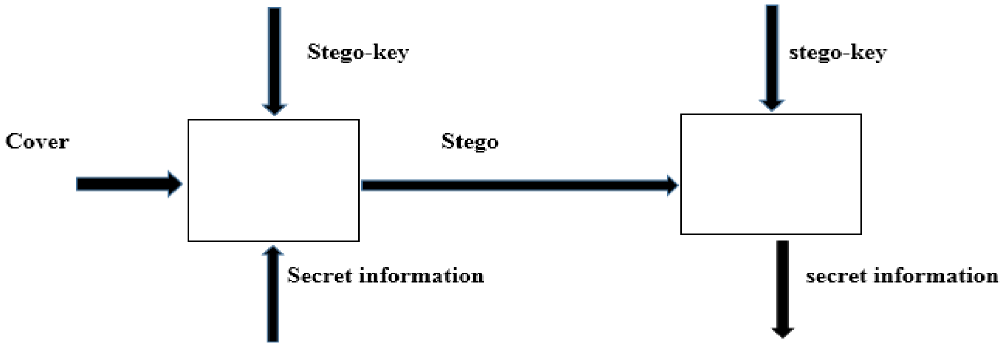


Figure 2.1 : Steganography process.

2.4 Uses of Steganography

With steganography you can send secret messages without anybody having knowledge of the existence of the communication. There are many countries where it is not possible to speak as freely as it is in some more democratic countries. Steganography can be a solution which makes it possible to send news and secret information without being censored and without the apprehension of the messages being intercepted.

While sending messages can be useful, it is also possible to simply utilize steganography to store information on a location. for instance, some information sources such as your private banking information, some military secrets and your medical images, can be stored in a cover source. When you are required to unhide the secret information in your cover origin, you can easily show your banking data and the recipe and it will be impossible to prove the presence of the military secrets inside. Steganography can also be used to perform watermarking. Although the concept of watermarking is not necessarily steganography, there are some of the steganography techniques that are being used for storage watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover image origin with extra information. Since communes will not accept noticeable alters in images, audio or video files because of a watermark, steganography technique can be used to hide this.

2.5 Implementation of Steganography

Secret messages can be hidden inside all types of cover information: text, images, audio, video and more. Most steganography utilities these days, hide information inside images Figure2.2 shows a basic form of a steganography system for embedding the secret image inside the cover image., as this is relatively easy to implement. However, there are tools available to store secrets inside almost any type of cover source.

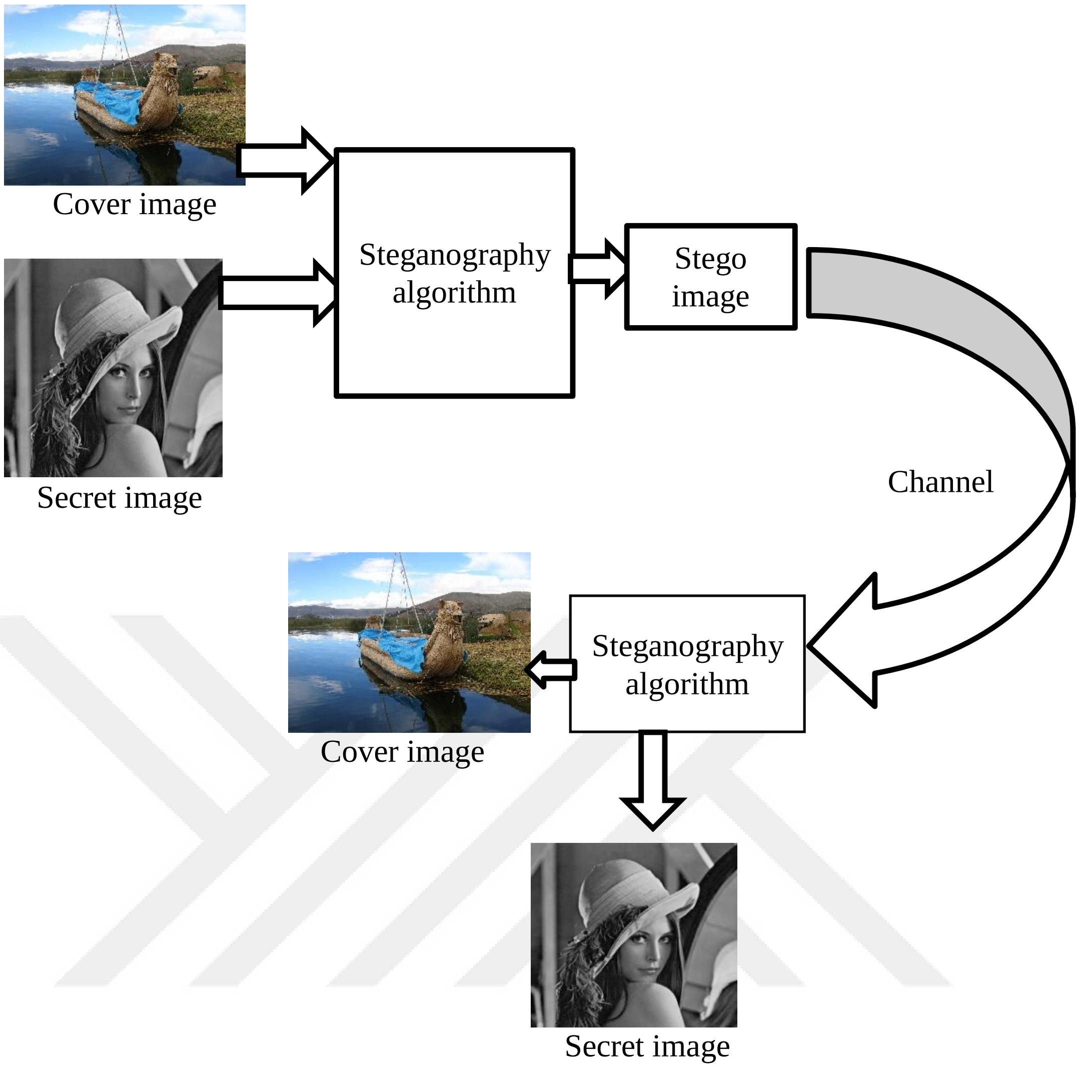


Figure 2.2 : A basic form of a Steganography system for embedding secret image inside cover image.

The most important property of a cover source is the amount of data that can be stored inside it, without changing the noticeable properties of the cover. When an image is distorted or a piece of music sounds different than the original, the cover source will be suspicious and may be checked more thoroughly [23].

2.5.1 Hiding a message inside a text

Since everyone can read, encoding text in neutral sentences is doubtfully active. But taking the first character of each word of the former sentence, you will see that it is possible and not very hard. Hiding information in plain text can be done by many various methods. The first-letter algorithm is not so secure, as knowledge of the system that is used, automatically gives you the secret. This is an abuse that many methods of hiding secrets into plain text have in common. Many techniques involve the modification of the mode of a text, rules such as using every n-th character or the altering of the amount of whitespace after lines or between words.

Another possible method of saving a secret message into a text is utilizing a publicly available cover source, a book or a newspaper, and using a code which consists for instance of a combination of a page number, a line number and a character number. This method, no information stored into the cover source will drive to the hidden message. Discovering it, relies solely on gaining knowledge of the secret key.

2.5.2 Hiding a message inside images

These days, it is very common to hide data inside an image and appear very easily in newsgroups by a German steganographic expert Niles Provost who invented a method to detect the presence of messages inside images. After testing a million images, no secret messages were found.The most popular methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image [24].

A-Least-significant bit modifications

The most widely utilized method to hide data is the usage of the LSB. Although there is some abuse of this approach, the relative easiness to implement it, makes it a popular method. To hide a secret message inside an image, a suitable cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, on the other hand, the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be utilized, also a total of 3 bits can be saved in each pixel. Thus, a 800×600 pixel image can include a total amount of 1,440,000 bits (180,000 bytes) of secret data. for instance, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory: (00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

In this case, only three bits required to be altered to insert the character successfully. On average, only half of the bits in an image will want to be modified to hide a secret message using the maximal cover size. The resulting changes that are made to the LSB are very small to be known by the human eye. Therefore, the message is effectively hidden. While using a 24-bit image gives a relatively big amount of area to hide messages, it is also possible to use an 8-bit image as a cover source. Because of the smaller space and different features, 8 bit images request a more careful way. Where 24-bit images use three bytes to represent a pixel, an 8-bit image utilize only one. Altering the LSB of that byte will create in a visible change of color, as another color in the available palette will be displayed. Therefore, the cover image requires to be chosen more carefully and preferably be in grayscale, as the human eye will not uncover the distinction between different gray values as easy as with different colors. abuse of using LSB alteration is mainly in the fact, so using these may rise suspicion. Another abuse will arise when compressing an image concealing a secret using a lossy compression algorithm. The hidden message will not survive and is lost after the transformation[24].

B-Masking and filtering

Masking and filtering techniques usually restricted to color image or grayscale image take different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be accomplished for instance by modifying the luminance of parts of the image. While masking does alter the visible properties of an image, it can be done in such method that the human eye will not observance the anomalies [23].

Masking techniques insert information in significant space so that the secret message is more integral to the cover image than just hiding it in the "noise" level [7, 23].

2.5.3 Hiding a message inside audio and video

Hiding information inside audio files can be done in several different ways, as modifications will often not create audible alters to the sounds. This method involves taking advantage of human limitations. It is possible to encode information using frequencies that are inaudible to the human ear. Using every frequency more than

20.000 Hz, messages can be hidden into audio files and will not be detected by human checks. Also, a message can be encoded utilizing musical tones with a substitution scheme. For entrance: F is tone will symbolize a 0 and a C tone symbolize a 1. A normal musical part can now be composed of the secret message or a present piece can be chosen together with an encoding scheme that will represent a message [23].

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the big amount of data that can be hidden inside and the fact that it is a moving stream of images and audios. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information.

2.6 Detection of Steganography

As more and more techniques of hiding information are developed and improved, the methods of detecting the use of steganography also advance. Most steganographic techniques involve changing properties of the cover source and there are several ways of detecting these changes [23].

2.6.1 Text

While information can be hidden in texts in such a method that the presence of the message can only be detected with knowledge of the secret key, for instance when using the earlier mentioned method using a publicly available book and a combination of character positions to hide the message, most of the techniques involve alterations to the cover source. These modifications can be detected by looking for patterns in texts or disturbing thereof, odd use of language and unusual amounts of whitespace.

2.6.2 Images

Detecting secret messages usually demands a more technical approach. Alter in size, file format, last changed timestamp and in the color palette might point out the presence of a secret message, but this will not always be the case. A widely utilized method for image scanning includes statistical analysis.

2.6.3 Audio and video

The statistical analysis way can be used with audio files too, there are some other things that can be detected, high unheard frequencies can be scanned for information and odd distortions or patterns in the sounds might point out the existence of a secret message. Also, variances in pitch echo or background noise might boost suspicion. Like implementing steganography using video files as cover sources, the methods of detecting hidden data are also a combination of techniques used for images and audio files .However, a different stenographic technique can be used that is especially effective when used in video films. The usage of particular code signs or gestures is so hard to detect with a computer system. This technique was used in the Vietnam War so an arrested person of war could communicate messages secretly through the video films the enemy soldiers made to transmit to the home front.

2.7 Relationship of Watermarking with Steganography

Watermarking is closely related to Steganography in that they are both concerned with covert communication and belong to a broader subject known as information hiding. However, the underlying philosophies of the two disciplines are different. Steganography is normally a point-to-point covert communication between two parties and a steganographic system is typically not required to be robust against the intentional removal of hidden message. Watermarking ,on the other hand, is usually a one-to-many communication and has the added notion that the hidden message should be robust to attempts aimed at removing it [25].

There exists a duality between watermarking (information hiding in general) and data compression. While compression aims to identify the perceptually insignificant parts of the data and remove them. Moreover, compression is one of the most common operations on images; therefore, one must take into account the effects of compression when designing a watermarking system.

2.8 Review of Fundamental Concepts Used in our Method

There are many methods that we used in our method, in this section we will review them.

2.8.1 Discrete wavelet transform

The transform of a signal is just another form of representing the signal. It does not alter the information content present in the signal. The Wavelet Transform gives a time-frequency representation of the signal. It was advanced to control the shortcoming of the Short Time Fourier Transform (STFT), which can also be utilized to analyses non- stationary signals. whereas STFT gives a steady resolution at whole frequencies, the Wavelet Transform uses the multi-resolution technique by which different frequencies are analyzed with various resolutions.

A wave is periodic an oscillating function of time or space. In contrast, wavelets are localized waves. They have their ability concentrated in time or space and are suitable for analysis of transient signals. While Fourier Transform and STFT utilize waves to analyze signals, the Wavelet Transform uses wavelets of finite energy. Figure 2.3 example of Haar wavelet.

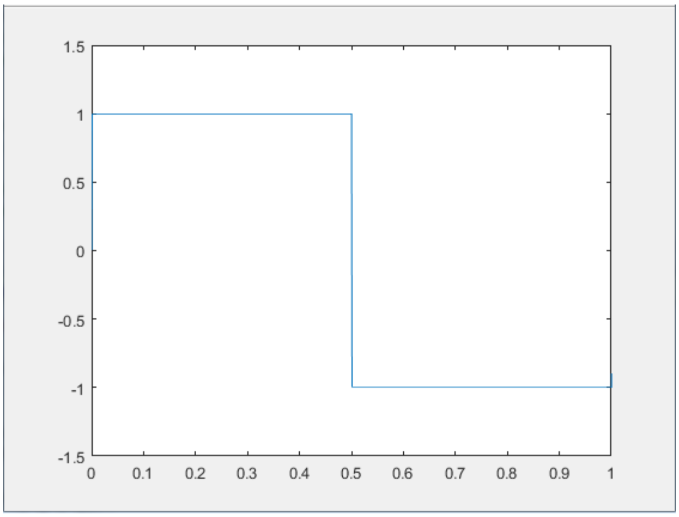


Figure 2.3 : Haar Wavelet.

The Wavelet Transform, at high frequencies, provides good time resolution and poor frequency resolution, however at low frequencies; the Wavelet Transform product perfect frequency resolution and poor time resolution [28, 29].

The Wavelet Series is just a sampled version of CWT and its computation may expend an important amount of time and resources, relying on the resolution wanted while (DWT), which is based on sub-band coding is found to yield a fast computation of Wavelet Transform. It is simple to perform and decrease the computation time and resources required.

The foundations of DWT return to 1976 when techniques to decompose discrete time signals were devised. Similar work was done in speech signal coding which was named as sub-band coding. In 1983, a mechanism like to sub-band coding was progressing which was named pyramidal coding. Later a lot of refinement was made to these coding system which resulted in active multi-resolution analysis schemes.

In CWT, the signals are analyzed utilizing a set of basic functions which relate to each other by easy scaling and translation. In the case of DWT, a time-scale representation of the digital signal is obtained utilizing digital filtering methods. The signal to be analyzed is passed through filters with various cutoff frequencies at different scales [28,30]. Figure (2.4) represent the process. we will use wavelet transform because the high frequency of wavelet that we can remove it by using threshold value is a lot, so wavelet transform give high capacity that means it can store many coefficients of secret information without effect on the clarity of the cover image, and PSNR of it very high. in my proposal I will use the 2D Haar wavelet decomposition. The Haar sequence was offered in 1909 by Alfred Haar. The Haar wavelet is as well so called as Db1, also the simplest possible wavelet.

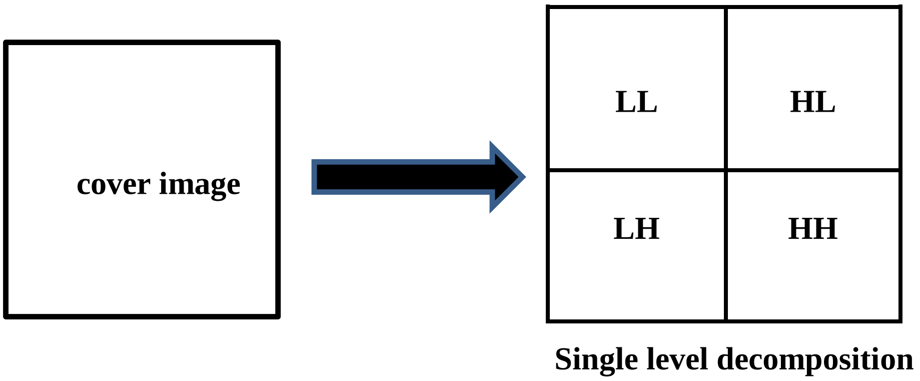


Figure 2.4 : Wavelet Transform Method of steganography system.

The Haar wavelet's mother wavelet function $\psi(t)$ can be described as [31]

$$\psi(t) = \begin{cases} 1 & 0 \leq t < \frac{1}{2} \ , \\ -1 & \frac{1}{2} \leq t < 1 \ , \\ 0 & otherwise \ . \end{cases} \tag{2.1}$$

Its scaling function $\phi(t)$ can be described as

$$\phi(t) = \begin{cases} 1 & 0 \leq t < 1, \\ 0 & otherwise \end{cases} \tag{2.2}$$

There are several important properties for this filter

1. The filter is reversible without the fear of affecting edge values while applying inverse wavelet.
2. In addition to its speed in a calculation and less memory usage.

2.8.2 Quad tree decomposition

There are numerous types of quadtrees that can be applied to any dimension, the notion is a repetition decomposition of space that makes us save only the significant or interesting information about the space. In this section, we will discuss 2-Dimensional quadtrees [32].

Quadtrees are utilized to split a 2-D space by recursively subdividing it into four regions (usually squares), this the process start by configuring the root node, so long as there is important data in the cell for which more iteration is desired, and the outcome is a tree data Hierarchal (a quadtree, where every node has four children). that means we can say that a very node in the tree denotes a cell [33,32]. The size of the quadtree relies on the complexity of the image.

This method will produce two type of quadrants a uniform and a nonuniform quadrant, and then every nonuniform quadrant is recursively split into four smaller subquadrants that are stored as four brother nodes of the quadtree [33,34]. We used the quadtree for easy decomposition in this technique, also it is the method to get the goal (decomposition) with few steps.

2.8.3 Fractal image compression

The fractal is one of the methods which was discovered in 1975 by Benoit Mandelbrot, occasionally referred to as the father of fractal geometry. He perceives that it is so often impossible to characterize nature utilizing only Euclidean geometry, that is in terms of straight lines, circles, diamond, and such like. He suggested that fractals could be used to describe real objects, like trees, mountains, river, to name but a few [35,33].

Recently, the fractal notion has evolved quickly not only in mathematics foundation but also utilized in a lot of research fields, particularly in signal and image analysis, for instance texture analysis of images for recognition, medical images analysis, and physiological signal processing and so on, and has accomplished remarkable success in numerous disciplines [33].

A mathematical fractal is based on an equation that succumbs iteration, a form of feedback established on recursion [33] is enough to create important transformations called affine transformations of the plane. Every can skew, stretch, rotate, scale and translate an input image. Figure 2.5 show examples of the fractal image. In our algorithm, we used the fractal image compression because it is a promising method to obtain high compression.

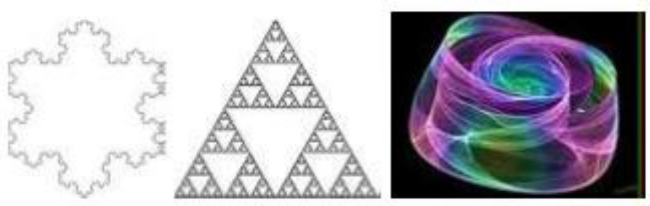


Figure 2.5 : Sample fractal images.

2.8.4 Huffman encoding

The Huffman compression algorithm is one of the most important file compression algorithms that operate at bit level, unlike the file compression algorithms that run at the byte level. The algorithm of Huffman encoding described by David Huffman, for the without loss compression of files rely on the frequency of the number occurrence of a symbol in the file that we want is compressed, it gives each symbol to a leaf node of a binary code tree [36].

The tree structure creates from joining the nodes step-by-step until all of them are put in a tree root. The algorithm always combines the two nodes that give the lowest frequency in a bottom-up step. The fresh interior nodes obtain s the total of frequencies of both child nodes [37,38].

The Hoffmann algorithm provides 20% to 90% of file size. Depending on the type of file itself, as the Hoffman algorithm works very efficiently and provides a lot of memory in the case of text files, but it does not affect the large image files and video files compared to text. [36] The amelioration of compression rates on the parameters of the affine transformations of the fractal compressed images is achieved by using Huffman encoding (lossless compression) [39]. Huffman algorithm to encode a stream of data efficiently. we used it to reduce the size of affine again ,in other words, it storage efficient of affine.

2.8.5 Huffman decoding

Any Huffman encoding relied on the probabilities of characters, these the frequencies will be written on the outcome and it can write the variable-length codes also on the outcome ,for this reason, will be very easy to apply Huffman decoding, because the frequencies will be integers.

Huffman decoding will start when it read the first bit of secret vector and then start to construct the Huffman tree, this the procedure starts from the root to bottom (the leaves of the tree) so that find the original. This process will be repeated for the next bit [33].

2.9 Peaks Signal-to-Noise Ratio (PSNR)

The Peak signal-to-noise ratio (PSNR) will be used to evaluate the quality of the stego-image after embedding the secret message, also to evaluate the quality of the extracted image after extracting.

The PSNR defined as follows:

$$PSNR = 10\log\frac{255^2}{MSE}db \qquad (2.3)$$

and mean square error

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j-0}^{n-1} (\alpha_{ij} - \beta_{ij})^2 \qquad (2.4)$$

where α_{ij} is the pixel of the cover image in the (i, j) coordinates, β_{ij} is pixel of the stego image in the (i, j) coordinate, (*m, n*) is the size of the cover image and stego-image [40].

2.10 The Structural SIMilarity (SSIM) index

This method can be used for measuring the similarity between two images.

$$\text{SSIM(x,y)} = \frac{(2\mu x \mu y + c1)(2\sigma xy + c2)}{(\mu x^2 + \mu y^2 + c1)(\sigma x^2 + \sigma y^2 + c2)} \qquad (2.5)$$

where µx and µy symbolize the mean values of x and y respectively. σx and σy are the variance of x and y respectively. σxy is the covariance of x and y. c1 and c2 are constants. The value of SSIM lies between [−1, 1]. A large value of SSIM points towards better quality [41].

2.11 Correlations

Correlation is the similarity test between the cover image and stego image. When the stego image is perceptually similar to the original cover image then the correlation equals one [42]. The correlation can be calculated as shown below:

$$Cor(c(r,c),s(r,c)) = \frac{\sum_{r=1}^{M} \sum_{c=1}^{N} (c(r,c) - \bar{c})(s(r,c) - \bar{s})}{\sqrt{\left[\sum_{r=1}^{M} \sum_{c=1}^{N} (c(r,c) - \bar{c})^2\right]\left[\sum_{r=1}^{M} \sum_{c=1}^{N} (s(r,c) - \bar{s})^2\right]}} \qquad (2.6)$$

where *r* is row number,*c* is column number, *M* is height of the cover-image, *N* is width of the cover-image, *c(r, c) is* cover-image, *s(r, c)* is stego-image, $\bar{c}$ is the mean of c(r, c) and $\bar{s}$ The mean of s(r, c).

3. THE PROPOSED METHOD SD-FIC

3.1 Introduction

Many secret images such as medical image and personal images are privacy of people that they do not want others see it ,and require high security when they are transmitted through the channel. In this research we suggest a safe and high resolution method for the secret image. We propose a steganography base method. The first phase is the embedding, by using the wavelet transformation for the cover image and calculate the threshold value, some of coefficients will become zeros. The secret image after applied fractal image and Huffman encoding of it, then embed it in the coefficients zeroes of wavelet inside cover image .

The second phase is the extraction. wavelet transformation decomposing is applied of the cover image, and the threshold is recalculated of the cover image and knowledge of the locations of zeros we can get the secret information, and then apply Huffman decoding and the fractal to reconstruct the secret image. the image was restored high resolution and the PSNR is acceptable when we compare it with other algorithms. In this chapter we will explain the proposed algorithm steps.

3.2 The Algorithm

The algorithm that we proposed is as following.

3.2.1 Objective

Is to propose a steganography system fast when processed in extraction, also suitable in capacity as high as possible inside the cover image to embed as much as possible.

3.2.2 Methodology

Since the information image must be preserved, therefore, this image in particular should be compressed using a lossless method or an accurate lossy method. On the other hand, the cover image must be tested for the available capacity which can be used to hide information. The measure for redundancy is suitable. There are several methods to test capacity:

- Testing entropy of the image.
- Testing compressibility using different methods[43], [44].
  - DCT transformation (expelling down almost a quarter of information stored in image without losing image readability)
  - Compression using wavelet.
- Detecting redundant information.

Remove the redundant information from the cover image to make space to embed secret image. Wavelet compression using zero-out method is one way to remove redundant information.

3.2.3 Testing performance

Steganography method finally is exposed to performance tests to evaluate the quality:

- PSNR test with the original image to test changes after embedding (between cover image and stego image), and extraction (between secret image and extracted image).
- Test manipulation attack (Rotating, resizing).

3.3 Encodıng Algorithm

Step 1- Finding of the entropy E(Ic)and E(Is).
Step 2- Discrete wavelet transform for cover image (DWT(Ic)) .
Step 3- Zero out certain threshold value for cover image after doing DWT.
Step 4- Fractal image compression for secret image by using Quadtree decomposition.
Step 5 -Huffman coding of parameters of the affine transformations H[.Affine={in , jn, dn, averagen}].
Step 6 - Embedding Is after step 5 in zeros of coefficients after step 3.
Step 7 – IDWT for the result for step 6.
Step 8 – The result is Stego image.
Figure 3.1 shows the summary of encoding algorithm.

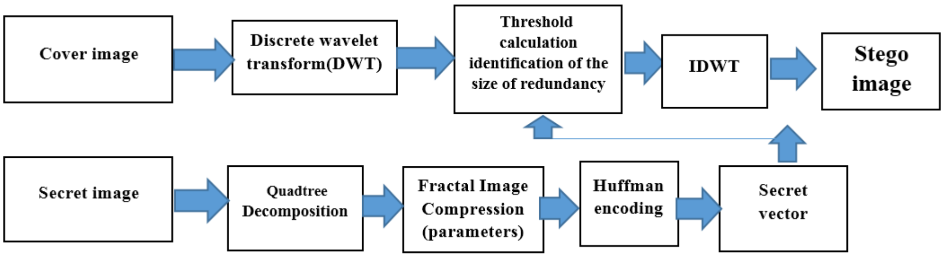

Cover image
Discrete wavelet transform(DWT)
Threshold calculation identification of the size of redundancy
IDWT
Stego image
Secret image
Quadtree Decomposition
Fractal Image Compression (parameters)
Huffman encoding
Secret vector

Figure 3.1 : The proposed steganography method for embedding.

Figure (3.2) shows example for embedding .

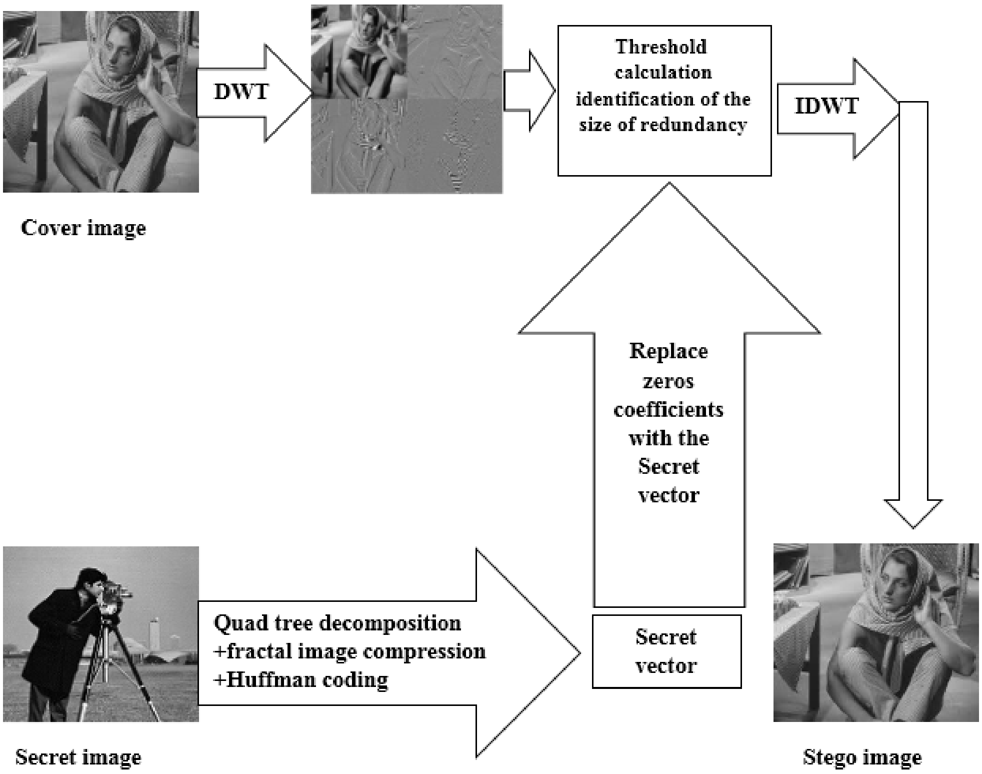

DWT
Threshold calculation identification of the size of redundancy
IDWT
Cover image
Replace zeros coefficients with the Secret vector
Quad tree decomposition
+fractal image compression
+Huffman coding
Secret vector
Secret image
Stego image

Figure 3.2 : Example for embedding stage.

3.4 The Embedding Phase

The first stage of our algorithm is the embedding that consists of these steps:

3.4.1 Entropy

Entropy E is the amount of information in the image that means how much information can be compressed without losing the ability to decode back the image.

If the entropy of the cover image E(Ic) is high, it means that there is a lot of significant information, in other words there will be a limit when the compression is applied. Means there is a relationship between the entropy E and the compression. If we work high compression, part of the image will be removed (part of the significant information) [46].

The error-free technologies are characterized by providing a high quality of the resulting images, but inability achieved a high compression rate of data. And the greatest compression can be achieved with this type determined by *Shannon's theory* which states that the rate of source information is determined by the entropy E according to the following equation [46].

Entropy is defined as

$$\mathrm{H}(x) = -\sum_{i=1}^{I} p(x_i) \log_2[p(x_i)] \tag{3.1}$$

where H(x) is the entropy E of cover Ic and secret Is images. $p(x_i)$ includes the histogram counts returned from image histogram of cover or secret image (Histogram: is a one-dimensional (vector) matrix, determines its color guide, and value. The array element specifies the number of pixels that carry this color in the image). $\log_2$ is the base-2 logarithm.

- The cover image Ic must be tested for the available capacity.
  - Finding entropy E for cover and embedded images.
  - If difference between cover image entropy E(Ic) and secret image entropy E(Is) is high, there will be a high chance of a successful embedding, since there would be a high chance to compress the secret and to remove high percent of the cover allowing more space for hiding.

Figure (3.3) demonstrate example of entropy, and Figure (3.4) example of histogram.

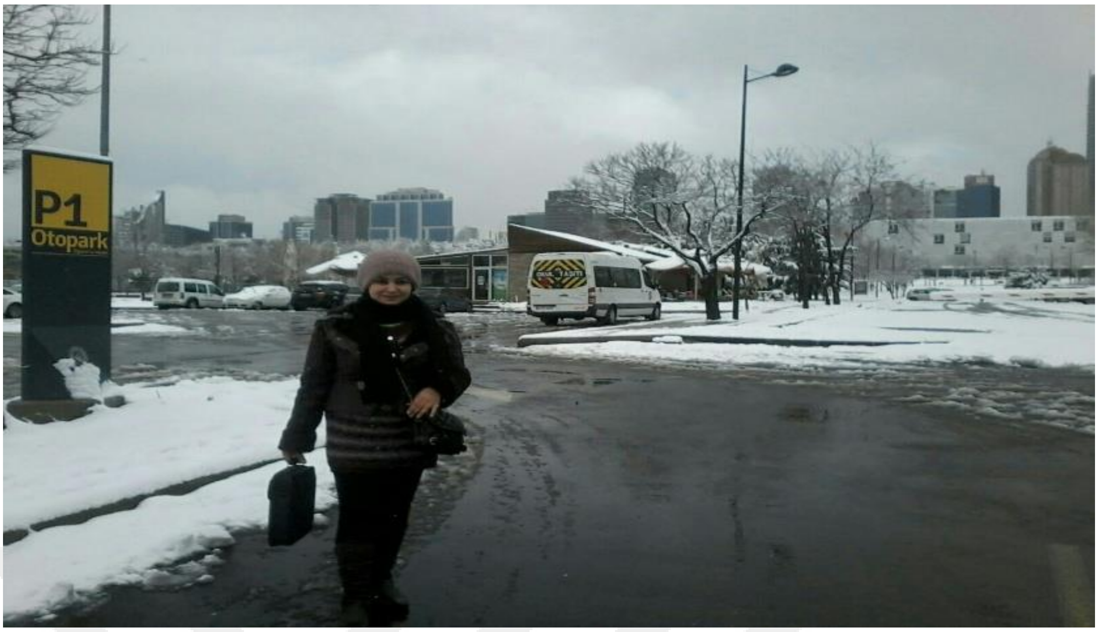


Figure 3.3 : Example of Entropy (rgb2gray ('suhad12.jpg')) =7.55 .

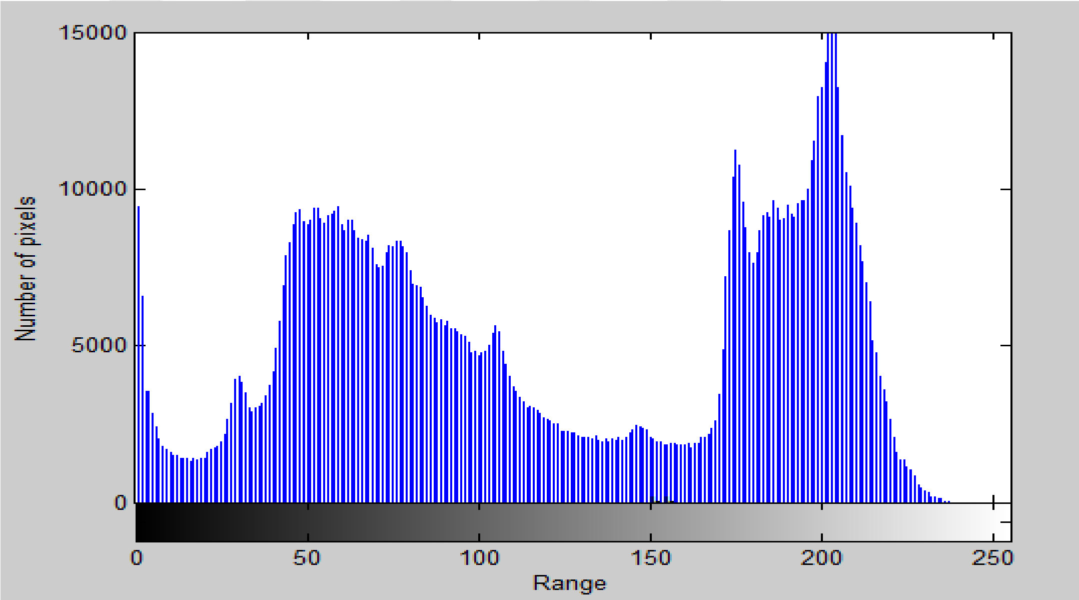


Figure 3.4 : Example histogram of suhad12.jpg.

3.4.2 The cover image Ic

In this section, we will explain algorithm of cover image Ic**.** The algorithm steps are as follows.

1. Discrete wavelet transform is applied to original cover image, DWT(Ic).
2. Calculate a threshold value using standard deviation and multiply the result with an Alpha α factor between (0-1).

3. Every coefficient value less than the calculated threshold value goes to zero.
   If xi < T → xi= 0.

3.4.2.1 Discrete wavelet transformation (DWT)

This technique works by taking wavelet transforms to encode a whole image DWT(Ic). As in figure (3.6). They allow images to be compressed so highly by storing the high frequency "detail" in the image separately from the low frequency parts. we applied this algorithm on a cover image Ic. The following Figure (3.7a) and (3.7b) example for represent the process to apply 2-D wavelet decomposition, level 1, haar filter bank coefficients on cover image Ic.

A- Direct method of computation.

In practice, the filter approach is the used for analyzing the signal frequency components. This consists of decomposing the signal into high and low frequency components. The information will be decomposed using haar filter. The DWT will is applied to the cover image as a following.

Step (1) Load the cover image Ic.

Step (2) It is high-pass filtered, resulting the three detail coefficients sub images (HL, LH, HH)

Step (3) It is then low-pass filtered and downscaled, resulting an approximation coefficients sub image (LL).

We used level 1 transformation ,therefore there is no need to repeat the decomposition.

The subband (LL) carries low frequency information which made it very noticeable part of the image. So we will not use this part to hide any information we do not include it in the threshold value scanning. [31]

Let an image d(x,y) of size L x H whose forward for discrete wavelet T(u,v,...)can be written in terms of the general relation:

$$\mathrm{T(u,v,...)}= \sum_{\mathrm{x,y}} \mathrm{d}(\mathrm{x},y)\mathrm{g}_{\mathrm{u,v}\ldots}\,(x,y) \tag{3.2}$$

where x and y spatial variables and u, v..... are transform domain variables, the $g_{u,v...}$ is called forward transformation [47,48]. The figure (3.5) shows 2 dimensional FWT the analysis filter

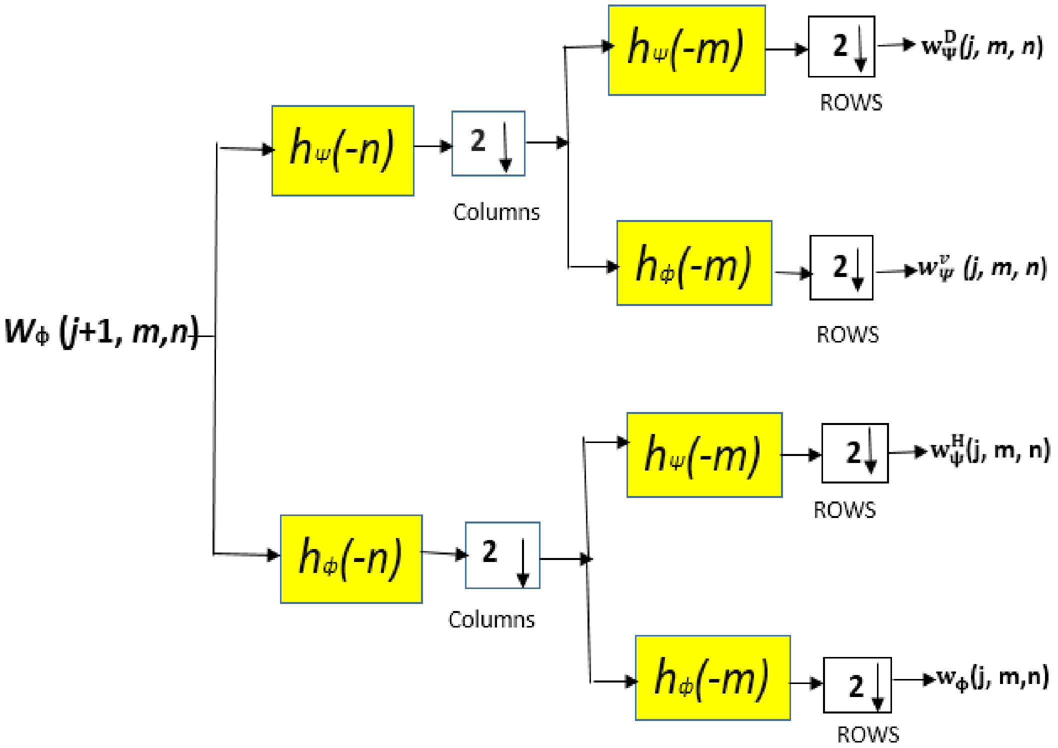
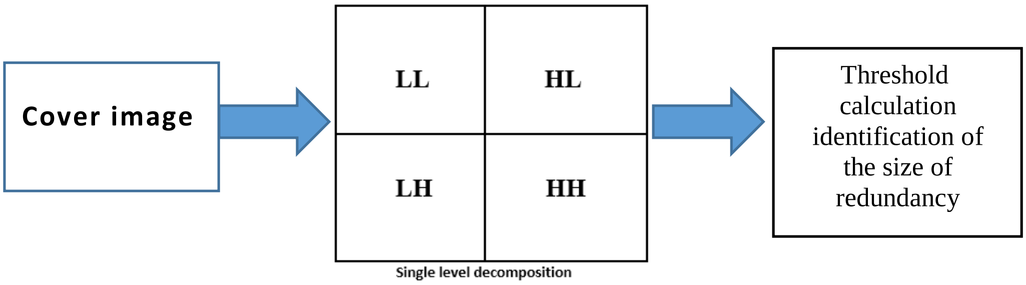


Figure 3.5 : The analysis filter bank of the two-dimensional FWT.



Cover image
LL
HL
LH
HH
Single level decomposition
Threshold calculation identification of the size of redundancy

Figure 3.6 : Wavelet transform method of steganography system.

Figure 3.7 : a) Original image, b) Subbands obtained by Discrete Wavelet Transform.

B-Keeping LL from any changes

After applying discrete wavelet transform for cover image DWT(Ic), and obtaining the wavelet coefficients, *xi*, where i =1, ..., N, and N is the total number of wavelet coefficients, appropriate alpha factor, α, will be selected between (0...,0.9) automatically. We will exclude (LL) for cover image as follows:

1. Taking copy of (LL) by taking half the size of the matrix of rows and half the size of the matrix of columns. In other words, take the first quarter of the image (LL) and store it temporarily away while replacing it with values more than the threshold value.
2. The threshold value for the (r, g, b) layers is then calculated separately.
3. Then selects the largest value (max (threshold value r, threshold value g, threshold value b) for the threshold. Taking the highest of them and use it on all layers.
4. Then we will multiply (LL) with ones matrix for this matrix the same size of LL, and multiply the result by max (threshold r, threshold g, threshold b).
5. compare coefficients value with the threshold value will be greater than the threshold value and in this way we have been excluded LL from any change.
6. The same steps mentioned above to keeping LL we will are applied to exclude HL from any change too.

C-Threshold value

1. The threshold value (*T*) is used to define what is the size (the space) of the redundancy in the cover image Ic that can be used to embed the message part in [16]. The input will be Alpha α parameter (0 -1).

2. Calculation of the threshold value is done via statistical standard deviation($\boldsymbol{\sigma}$).

$$\boldsymbol{\sigma} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2} \qquad (3.3)$$

$$T = \alpha \qquad (3.4)$$

3. if the value of the wavelet coefficient is less than the threshold value, xi<T, then enforce that particular coefficient to take the value zero, xi =0.

where α is The Alpha factor is between 0 and 1.

3.4.3 The secret image Is

In this section we will explain algorithm of secret image(Is**).** The algorithm steps are as follows.

1. Splitting the original secret image (Is) by utilizing Quad tree decomposition we will use certain threshold value.
2. Saving the values of (x ,y) coordinates, average value and block size the results from Quad tree Decomposition.
3. Record the fractal coding data (affine transformations).
4. Encoding parameters resulting from applying the fractal image by using Huffman encoding [33].

3.4.3.1 Quadtree decomposition

The primary issue is that the fractal encoding is taking a lot of time. Many ways to deal with lessen the encoding time has a bad influence on the image quality after repetition, hence the hybrid encoding technique for joining fractal coding and other coding strategies turns into leading direction of fractal techniques ,for this reason, we will use Quadtree first.

Generally, the use of fractal here depends heavily on the Quad tree decomposition of the images to find affine transformations depending on the mean value for each affine.

Quadtree decomposition is an analysis method that includes subdividing an image into blocks that are more identical than the image itself. It is additionally valuable as the initial phase in compression algorithms.

1- Splitting a square image into equal four quarters blocks.

2- Examining each block to check whether it meets some foundation of homogeneity (e.g., if every one of the pixels in the square is inside a particular dynamic range). In our algorithm, we calculate the average intensity of pixels and compare it with the threshold value of Quadtree.

In the condition that a square meets the standard (threshold value), it is not partitioned further. however, if it didn't meet the standard, it will be subdivided once more into four blocks, and the test rule is utilized for those squares. This procedure is repeated until each the block meets the model. The outcome may have block of a few distinct sizes [49]. The following graph figure (3.8) represent the process.

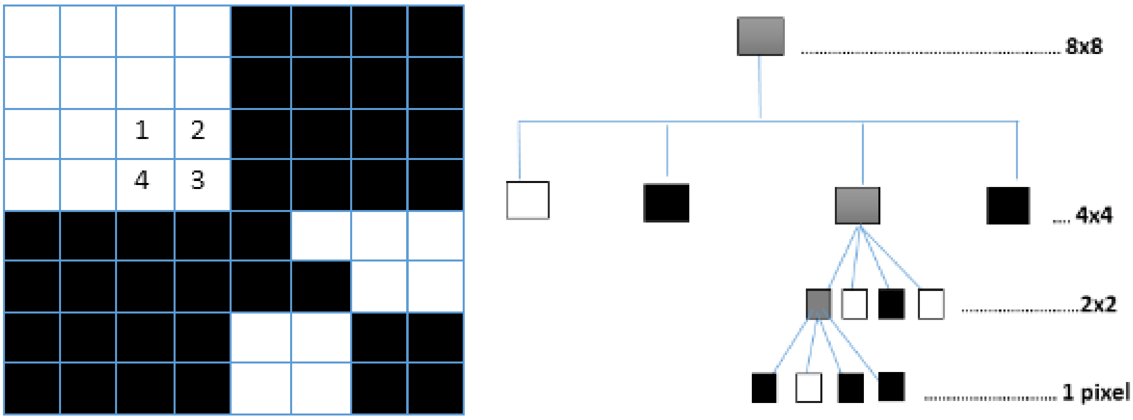


Figure 3.8 : Example clarify the quad tree.

To understand this part of the decomposition let us consider an example of small image 64×64.as in figure 3.9.

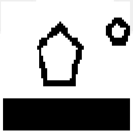


Figure 3.9 : Small image 64×64.

This image is created using paint saved as PNG and scaled to be grayscale in MATLAB

It’s been thresholded on 0.2 value and decomposed with minimum block dimension 2×2 and maximum 16×16 blocks. The result comes to be as in figure 3.10.

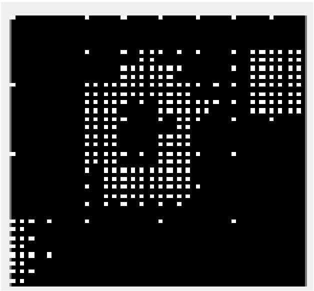


Figure 3.10 : Decomposition with 0.2 threshold value.

Figure 3.11 show decomposition with 0.7 threshold value and with minimum block dimension 2×2 and maximum 16×16, while Figure 3.12 demonstrate decomposition with 0.2 threshold value and with minimum block dimension 4×4 and maximum 16×16, and Figure 3.13 show decomposition using 0.7 threshold value minimum 4×4 and maximum 16 ×16 block size.

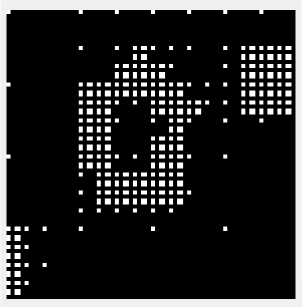


Figure 3.11 : Decomposition with 0.7 threshold value and with minimum block dimension 2×2 max 16×16.

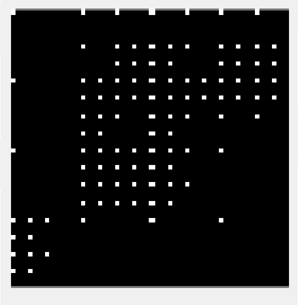


Figure 3.12 : Decomposition with 0.2 threshold value and with minimum block dimension 4×4 max 16×16.

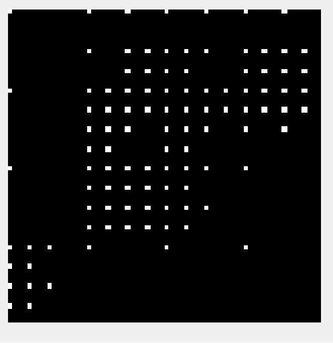


Figure 3.13 : Decomposition using 0.7 threshold value min 4×4 and maximum 16×16 block size.

One can notice the effect of the minimum block size affected on the degree of details, while the threshold value affects only the contrast level of information it has no significant effect on the type of image in the example.

If we took the largest maximum size block, the result will be more information is taken into account and a smaller tree is going to be created.

The figure(3.14) and(3.15): shows an example of an application the Quadtree.

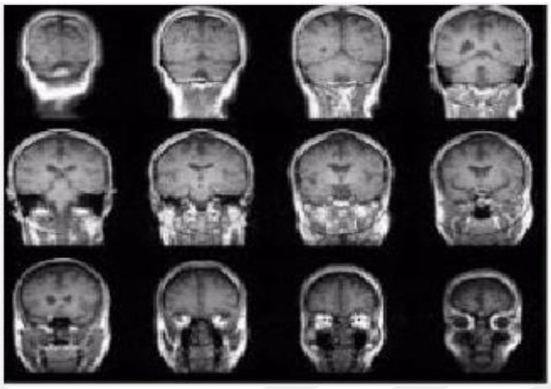


Figure 3.14 : Original secret image.

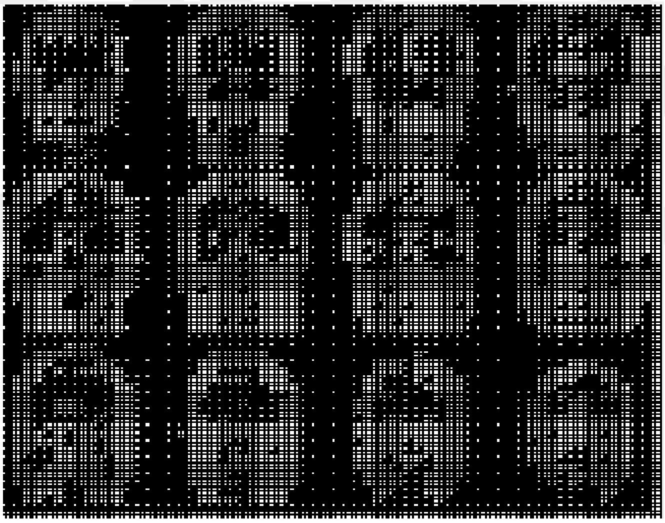


Figure 3.15 : Quadtree for secret image.

3.4.3.2 Fractal image compression

We can get Fractal image compression FIC by dividing secret image Is into non overlapping blocks rely on a threshold value and the renowned methods of Quad tree decomposition [50]. Then it begins to calculate the mean for each block to build the affine transformation .The affine is formed characteristic for the smallest block this form is repeated by modification under a certain system for example in our case here is the mean. The result is a numeral from parameters [50].In this case, the quadtree and fractal are overlapping in other words directly after dividing the block, calculate the average and compare it with threshold value.If meet the condition, the fractal image compression will compress the block(for example if the block was 64x64 and it satisfies the condition, after applying FIC, will use only 8 bytes (2 bytes for i, 2 bytes for j,2 bytes for d 2 bytes for mean).

1. Will be taken the mean for image parts for all blocks found to start at image location(i, j) with a dimension of block size d and store it.
2. The result will be group from Affine transformations (1.... n) ={in , jn , dn , averagen}

where i is row value, j is column value and d is dimension of the block size.

3.4.3.3 Hufmann coding of the parameters

The outputs from applying the fractal are parameters (affine transformations). These parameters are further compressed via a Huffman-encoding scheme. thus, the affine becomes in the form of numbers.

The Huffman encoding algorithm begins by building a roster of all the symbols in downward order of their probabilities. It then builds, from the base up, a binary tree with a character at each leaf. This is done in steps, where at each progression two characters with the littlest probabilities are chosen, added to the highest point of the fractional tree, omitted from the roster, and supplanted with a helper symbol substituting to the two main symbol [51]. At the point when the list is diminished to only one helper symbol (representing to the whole alphabet), the tree is finished. The tree is then traversed to define the code words of the symbols [33].

3.5 Embedding Secret Information Into the Decomposed Cover Image

After compressing secret image information with Huffman code its necessary to store the data in a special way because the output of the encoder is a stream of 1’s and 0’s, hence the stream must be converted to 8-bit groups and store them in memory location normally as 8-bit binary numbers. In addition, the code dictionary which it is needed for the decoding process also must be stored. Again the dictionary is a group of 1’s and 0’s changing in length depending on the code generated which in turn is a representation of the probability of the data symbols in the secret image affine.

Affine are extracted from the fractal image compression technique used earlier. A necessary piece of information is how long the stream is going to be and is it divisible over 8 without a remainder, if so another byte (8 bit) is added to bytes, vector containing the binary stream specifies the number of zero bits added to complete the stream and make it divisible by 8 without a remainder. Which means if there is no remainder this byte contains zero. The byte is added after encoded data and the dictionary. The group of information is called the Secret vector.

Then Secret vector is rescaled (to get the highest PSNR for the cover image versus the stego image, in other words to obtain on stego image be very similar to the cover image, so we divide all secret vector over its maximum value, and multiply it by threshold value,maximum value is equal or less than threshold value of wavelet, so when inverse of wavelet is made, the cover image will remain without changes or contain few of them) and embedded into the zeroed wavelet coefficients. The rescaling should be covering a condition must not exceed the threshold value, so it can be calculated later on.

3.5.1 Replacing the zeros coefficients for the cover image with secret vector

After applying DWT (Ic) and finding the *T* [DWT (Ic)] .Also finding the Quadtree, fractal and Huffman encoding(Is), then we can embed the secret image in the cover image by replacing the zeros coefficients to cover image (after DWT and finding the threshold value) with results appearing after Huffman encoding. If DWT (Ic(x_1), Ic(x_2), Ic(x_3), ..., Ic(x_n). < T, then (Ic(x_1), Ic(x_2), Ic(x_3), ..., Ic(x_n). will replace with Secret vector (secret information).

3.5.2 IDWT after embedding the secret image inside the cover image

After embedding the secret image (after applying the proposed algorithm for the secret image) in the cover image (after applying the proposed algorithm for the cover image) we will apply an inverse discrete wavelet transform for result. this process performs a single-level two-dimensional wavelet reconstruction by particular wavelet reconstruction haar (db1) filter that we specified**.**

3.6 Decoding Algorithm

1- Decomposing stego image into sub bands using wavelet transform(2-D wavelet decomposition, level 1, Haar filter).

2- Extracting used threshold value(it is stored in determined locations inside stego image)from stego image. Should be the same or in the same range when calculated.

3- Finding insignificant coefficients (if coefficient value < threshold valve).

4- Collecting the values of zero coefficients(The values of the Secret vector which were replaced with zeros coefficient for cover image).

5- Huffman decoding of Secret vector .

6- Decode affines parameters.

7- Iterating to build fractal decomposed secret.

Figure 3.16 The summary of decodıng Algorithm.

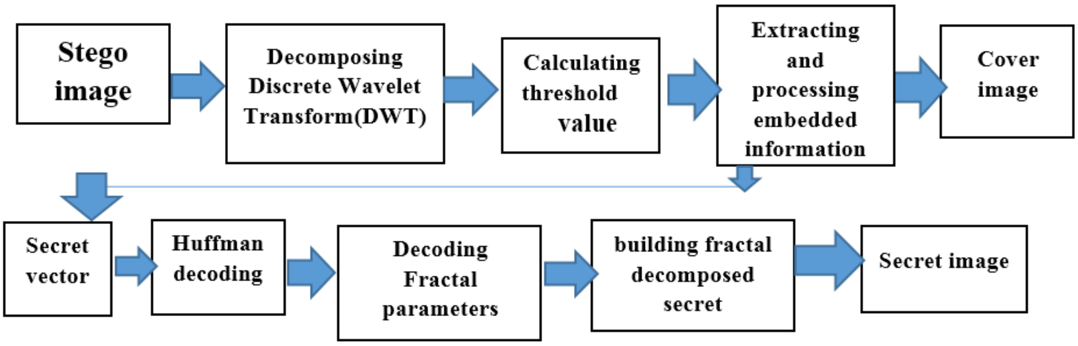

Stego image
Decomposing Discrete Wavelet Transform(DWT)
Calculating threshold value
Extracting and processing embedded information
Cover image
Secret vector
Huffman decoding
Decoding Fractal parameters
building fractal decomposed secret
Secret image

Figure 3.16 : The proposed steganography method for extraction.

Figure (3.17) shows example for extraction.

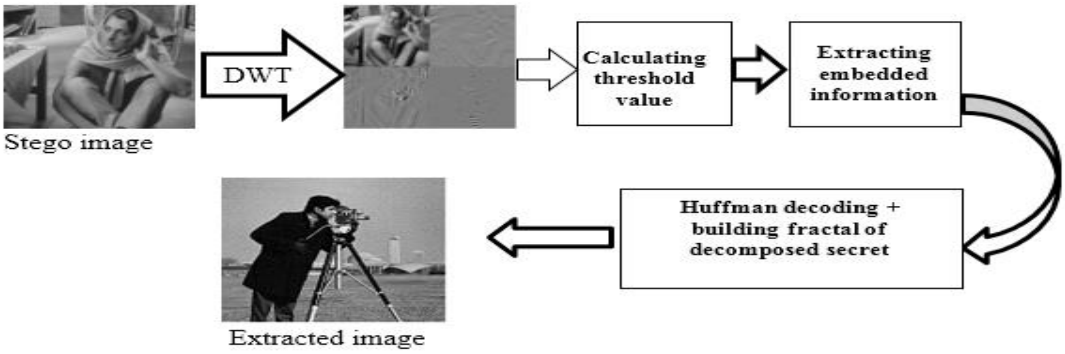

DWT
Stego image
Calculating threshold value
Extracting embedded information
Huffman decoding + building fractal of decomposed secret
Extracted image

Figure 3.17 : Example of the proposed steganography method for extraction stage.

3.7 The Extraction Phase

The cover image Ic decomposed using discrete wavelet transform. Threshold value is calculated for the wavelet coefficients DWT(Ic). Then a search for insignificant coefficients ($xi<T$) is started. The same threshold value should be guaranteed to find

the same locations where we stored our Secret vector sv. When the vector is found ,the vector is rescaled back to its normal value by dividing it with the threshold value then multiply it with maximum value which is stored at the highest location of the wavelet to spread the value over the entire range and analysis of the vector is started to extract Huffman code data and retain it to its first shape as a binary stream and then extract the dictionary which is also an array of binary bits stored each group in a cell where it corresponds to the symbol has been coded with. A Huffman decoding is executed. Then just after this step, the fractal image iterations is started to rebuild the secret image as close as possible to the real image.

4. RESULTS AND DISCUSSION

4.1 Introduction

In the previous chapter, we explained the procedure for the process of steganography, to give high security to hidden data (secret image). The process of steganography has been well, so it did not give a large difference between the cover image and the stego image when we calculate the difference by using correlations for determining the similarity for the two images. In addition, it gave high PSNR between the cover image and the stego image, also between the original secret image and the extracted image. In this chapter contains the results and the assessment of the tests.

4.2 Dataset

It is necessary to define the data set, where every measurement was taken and studied. The following tables show according to the type of image whether its grayscale or colored.

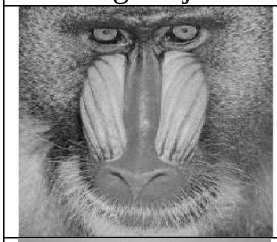
4.2.1 Secret images

Secret images can be any size in reality. But here small sizes taken to overcome the limitation of hardware were calculations take a long time to execute, while the relative results are the same for studying. A group of grayscale and colored images to follow:

4.2.1.1 Grayscale images

Grayscale images relatively have small size than its colored version since colored stores information for red, green and blue layers. Table 4.1 shows grayscale secret images used.

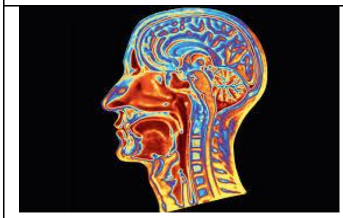
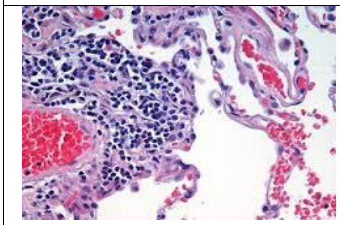
Table 4.1 : Grayscale secret images used in tests.

Image object	File name	Size
	babbon.jpg	256×256
	cameraman.jpg	256×256
	image15-gray.jpg	262×192

4.2.1.2 Color images

Table 4.2 shows colored secret images used in tests.

Table 4.2 : Colored secret images used in tests.

Image object	File name	Size
	Images.jpg	275×183
	Pepper1.jpg	256×192
	a.jpg	240×178

4.2.2 Cover images

Cover images must be larger in size to host secret information. Table 4.3 shows some of the cover images used.

Table 4.3 : Cover images used in tests.

Image object	File name	Size
	London-Eye-night.jpg	2592 × 3872
	Reed_Islands_of_Lake_Titicaca_-b.jpg	3072 × 2304
	Chrysanthemum.jpg	768 × 1024
	Bird.jpg	512 × 512

4.3 Compression vs Entropy

E Entropy represents the amount of information contained within the digital image. While there is little information available it is obvious to the observer that compression ratio increases with the decrease of entropy measure of the digital image. The entropy measures the efficiency of encoding.

4.3.1 Grayscale images

Table 4.4 shows compression possibilities according to entropy and actual compression using a hybrid of Huffman and fractal decomposition to produce a Secret vector can be stored and extracted later. The results show the compression was between 48% to 72% [52]in spite of changing entropy from 2.1 – 7.18 bit/pixel.while efficiency encoding was between 111% to 371 [46,52,53].

$$\text{Compression ratio(real)} = \text{uncompressed data rate/compressed data rate.} \tag{4.1}$$

$$\text{Efficiency encoding(expected)} = 8\text{bit}/E \ . \tag{4.2}$$

Table 4.4 : Compression using gray scale images.

Secret Image	Entropy	Compression	Efficiency encoding	Total
babbon.jpg	7.1819	0.48409	111%	48%
cameraman.jpg	7.1047	0.72516	113%	72%
image15-gray.jpg	2.1588	0.60771	371%	60%

4.3.2 Color images

Color images show even less total compression ratio because of a large amount of data stored. It's notable the change between babbon.jpg and image15—gray 111%-371% encoding efficiency according to the entropy which gives 48% and 72% of real compression while in color images as seen in Table 4.5 132%-533% compression efficiency is expected according to entropy while actually 51% to 103% is calculated.When we compare with grayscaled we can note the change is higher than grayscale. Which means there are other parameters affects the efficiency and it is related to color and size of the image.

Table 4.5 : Compression using colored images.

Secret Image	Is Entropy	Compression ratio	Efficiency encoding	Total
a.jpg	5.78846	0.51072	138%	51%
images.jpg	1.49974	1.033	533%	103%
Pepper.jpg	6.05620	0.79223	132%	79%

Since the compression method uses both fractal decomposition (which in turn uses quad tree as a method of decomposition) and Huffman encoding to encode the resulted affine, it is important to show the effect of Quad tree decomposition threshold value upon the compression ratio. Table 4.6 shows a change of compression ratio in spite of fixed entropy according to the threshold value of Quad tree decomposition. This is because when the threshold value is decreased expectancy to produce more detailed blocks increasing the number of affine elements which affects the encoding efficiency in total.

Table 4.6 : Entropy, compression vs quad tree threshold value.

Image	Entropy	Compression	Threshold value
cameraman.jpg	7.10477331	106%	0.05
cameraman.jpg	7.10477331	93%	0.03
cameraman.jpg	7.10477331	83%	0.02

The Compression is actually independent of the cover image because the whole operation is done until a Secret vector is produced without having the cover image in the process. While this process is independent of the cover image but still the output of the process is related to many aspects like the number of locations we can use inside the cover image without disturbing it. As long as a short secret vector is produced a high chance of selecting a variety of covers with success hiding.

The use of Huffman only as a method of compression shown in Table 4.7 where the theoretical compression efficiency according to the entropy is without any changing while real compression is widely changing. The table also shows two rows grayscale images as can be seen from that second row of the table is mostly black while cameraman image is somehow different and mostly filled with details allowing fewer possibilities to find similar data to encode and thus compress as it can be noted a lower entropy allows more compression than cameraman image.

Table 4.7 : Entropy vs compression using Huffman method.

Image	Entropy	Efficiency	Compression
cameraman.jpg	7.10477331	113%	111%
image15-gray.jpg	2.158830549	371%	322%

Entropy as a measure shows how much this image can be reduced in an encoded version, hence shows for the secret image how much the image can be compressed, and how much for a cover image can hold redundant information, although this is not accurate but it gives the idea of the suitable relation between the secret and cover images. Sometimes the embedding process succeeds even though secret entropy is larger than cover entropy, this is because there are differences in sizes and the available space is enough for hiding. Nevertheless, the chance is always high when there is a large difference between the two.

4.4 Embedding Efficiency

Important to measure the embedding efficiency because this indicates what kind of cover image can be used to what kind of image we intend to hide. Efficiency can be measured taking account of many aspects though every hiding method has its own aspects to consider.

4.4.1 Size ratio

Successful embedding operations require a very important condition is that the size of the cover is larger than the size of the embedded image. While this is a true fact it is important to study the limits of the type of image both the secret and cover images to have a successful embedding. This is related to the amount of compression the secret image that is allowed , and the amount of redundant information can be used as storage locations for the compressed secret image without the cover image is deteriorated. This allows slight change of sizes according to the type of image used although the method used casts some conditions like the size of the secret should be square and power of two this is considered a drawback, nevertheless, the size added is simply compressed using the hybrid method overcome the additional space in a reasonable size Table 4.8 shows the ratio of embedded images. The image in the last row is under size when squared and a power of two is made, but the compression depend upon the nature of the secret and cover images.

Table 4.8 : Size ratio for successful embedding operations.

Cover Image	Original Size	Width	Height	Ratio(Is/Ic)
London-Eye-night.jpg.jpg	2592 x 3872	2592	3872	
Secret Image				
cameraman.jpg	256 x 256	256	256	1%
image15-gray.jpg	262 x 192	512	512	2%

There is some freedom in finding redundant data in a cover image and remove them. This operation is made as described in chapter three using threshold value of wavelet technique. Thus the number of locations can be used is determined by the nature of the image used as a cover.We can compare the space saving(real) with redundant information(expected) [46,52,53].

space saving(real)= 1- (compressed data rate/ uncompressed data rate). (4.3)

redundant information(expected)= 1- (E/8bit) (4.4)

Table 4.9 : Cover capability to store information.

Image	Entropy (b/pixel)	Width	Height	Redundant information (1-entropy/8bit)	Amount can be used (pixel)
London-Eye-2009.jpg	7.582129418	4272	2848	5%	635510.953
Chrysanthemum.jpg	6.167719742	1024	768	23%	180120.4785
London_Eye_Night_Shot.jpg	6.593029588	3872	2592	18%	1765083.777

4.4.2 Effect of alpha factor

Alpha factor is a parameter used to scale up and down the values of the secret coefficients to hide within the wavelet coefficients without disturbing the original cover image after inverse wavelet, also to be persistent and recoverable after decomposition. The alpha factor plays important role a several tries is used in a loop to find suitable alpha before embedding. Although many tries are allowed its notable that a small range of alpha is usually successfully which it is perhaps back to the nature of the images both cover and secret. Figure 4.1 shows how PSNR values affected by Alpha for the same cover and different secret images. While the graph shows clearly there is no direct relation to the PSNR although it was a successful embedding.

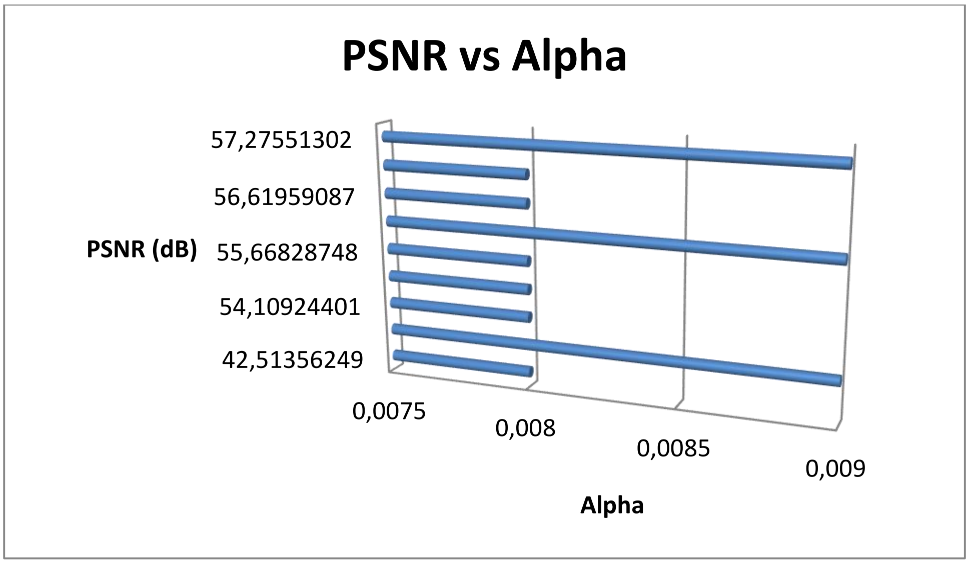


Figure 4.1 : PSNR of Stego vs selected alpha.

4.4.3 Embedding speed.

Embedding speed depends on several parameters. But most important one is how deep the compression is. As the compression is higher the processing time is higher. Although, size also affects the speed of processing as it cast shed over the number of coefficients must be taken and replaced.

4.5 Extraction

The second part of the results is the extraction phase where the secret must be found extracted out of the cover image and decoded back to the original image. Certainly there are several measures to consider for the successful extraction.

4.5.1 Quality

Quality of the extracted image is important since the information must be retained without change or a slight change can be tolerated at the receiver side. Quality of the image can be measured depending on PSNR between original secret and the extracted secret and also be calculating the entropy difference between original and extracted secret which can show how much of the information is lost. Figure 4.2 shows cameraman image in two different cases where encoding depends on the threshold value where the first case has higher threshold value allowing to have higher information loss hence lower PSNR, while the lowest difference between the entropy of original and extracted gives higher PSNR , hence high quality of the image.

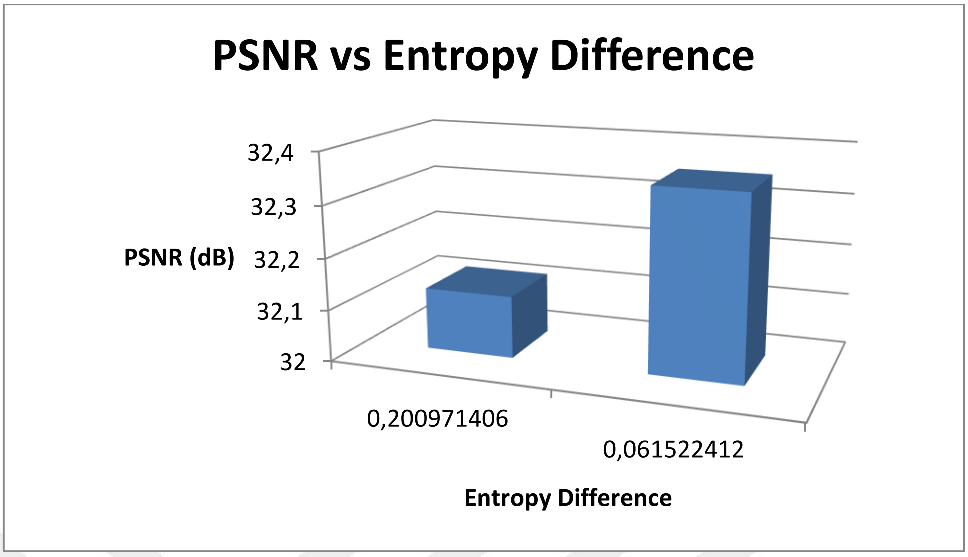


Figure 4.2 : Entropy difference affects PSNR and hence Quality.

4.5.2 Speed

Extraction speed depends entirely on the amount of information embedded. Figure 4.3 shows time taken to extract a secret image from stego images since it contains a higher amount of information it is reasonable to take longer to extract. This also applies to lower entropy values since it requires a longer time to decode the encoded secret. The measurement is taken for the same image with different PSNR values.

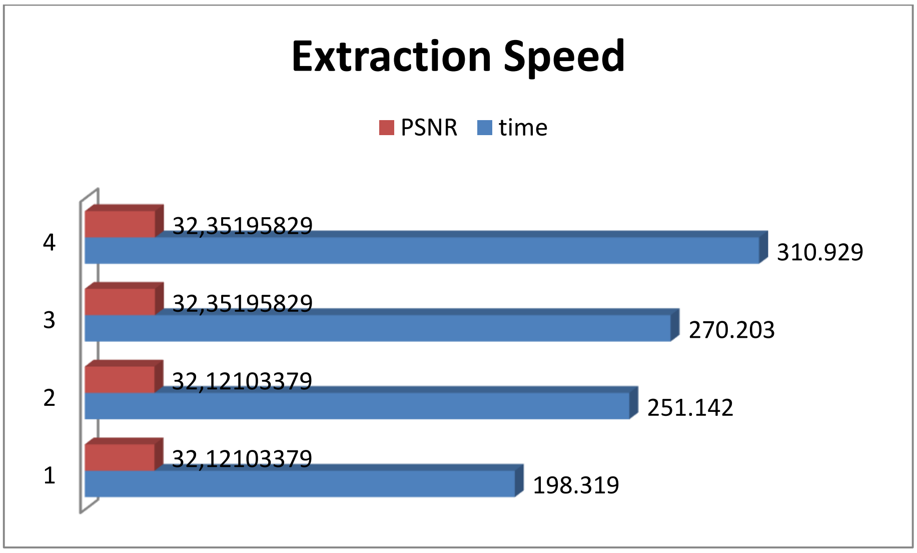


Figure 4.3 : Extraction speed depends on amount of information embedded PSNR vs time in seconds.

4.6 Secrecy

The secrecy of the stego image is compromised when a cover image appears to be unnaturally disturbed .A high correlation values between the original cover and the stego image and high PSNR gives the impression of there is no manipulation of the cover image . A high correlation values are gained for successful image hiding. Table 4.10 shows high correlation with reasonable PSNR between cover image and stego image for both grayscale and colored secret images.High correlation makes it difficult for human eyes to detect any changes in the cover image.

Table 4.10 : Correlation and PSNR between Cover and Stego for different secret images.

Cover image	Secret image	PSNR Cover image vs stego	Correlation
Chrysanthemum.jpg	images.jpg	44.8337	0.9994
Chrysanthemum.jpg	image15.jpg	44.4844	0.9998
Chrysanthemum.jpg	a.jpg	43.6983	0.9992
Lighthouse.jpg	cameraman.jpg	43.2729	0.99992
Lighthouse.jpg	image15.jpg	42.8431	0.99998
Chrysanthemum.jpg	cameraman.jpg	45.4023	0.99998
London-Eye2009.jpg	cameraman.jpg	65.61959	1
London-Eye2009.jpg	image15gray.jpg	56.67228	1
Reed.jpg	Babbon.jpg	55.8919	1
Reed.jpg	Pepper.jpg	55.6396	1

4.6.1 Secret vector hiding

The Secret vector is positioned inside a wavelet decomposed image using a threshold value which mostly takes the decomposed image column wise scanning its coefficient for under threshold values which they are scattered in the sub bands of the decomposed wavelet image. This is certainly very difficult way to scatter the parts of the vector stored in a special format and encoded, since the positions which satisfies the condition depends directly on the cover image while the content of the secret vector depends entirely on the secret itself.

4.6.2 Extracted image vs original secret image

As can be seen from Table 4.11 the PSNR values are acceptable for the secret extracted although when compared to extraction using Huffman method gives infinity PSNR. This results depends on the fractal method used here we used averaging method to identify characteristic fractal or basic fractal element.

Table 4.11 : Extracted vs original secret PSNR.

Cover image	Secret Image	PSNR
Lighthouse.jpg	cameraman.jpg	34.0789
Reed.jpg	Babbon.jpg	35.3729
Chrysanthemum.jpg	image15.jpg	39.2368
Chrysanthemum.jpg	images.jpg	31.1960
Chrysanthemum.jpg	a.jpg	30.0659
Reed.jpg	Pepper.jpg	36.007

4.7 Examples

Table 4.12 shows some of cover, secret, stego and extracted images, Table 4.13 shows some of results of embedding and extraction processes .

Table 4.12 : Examples of embedding and extraction processes.

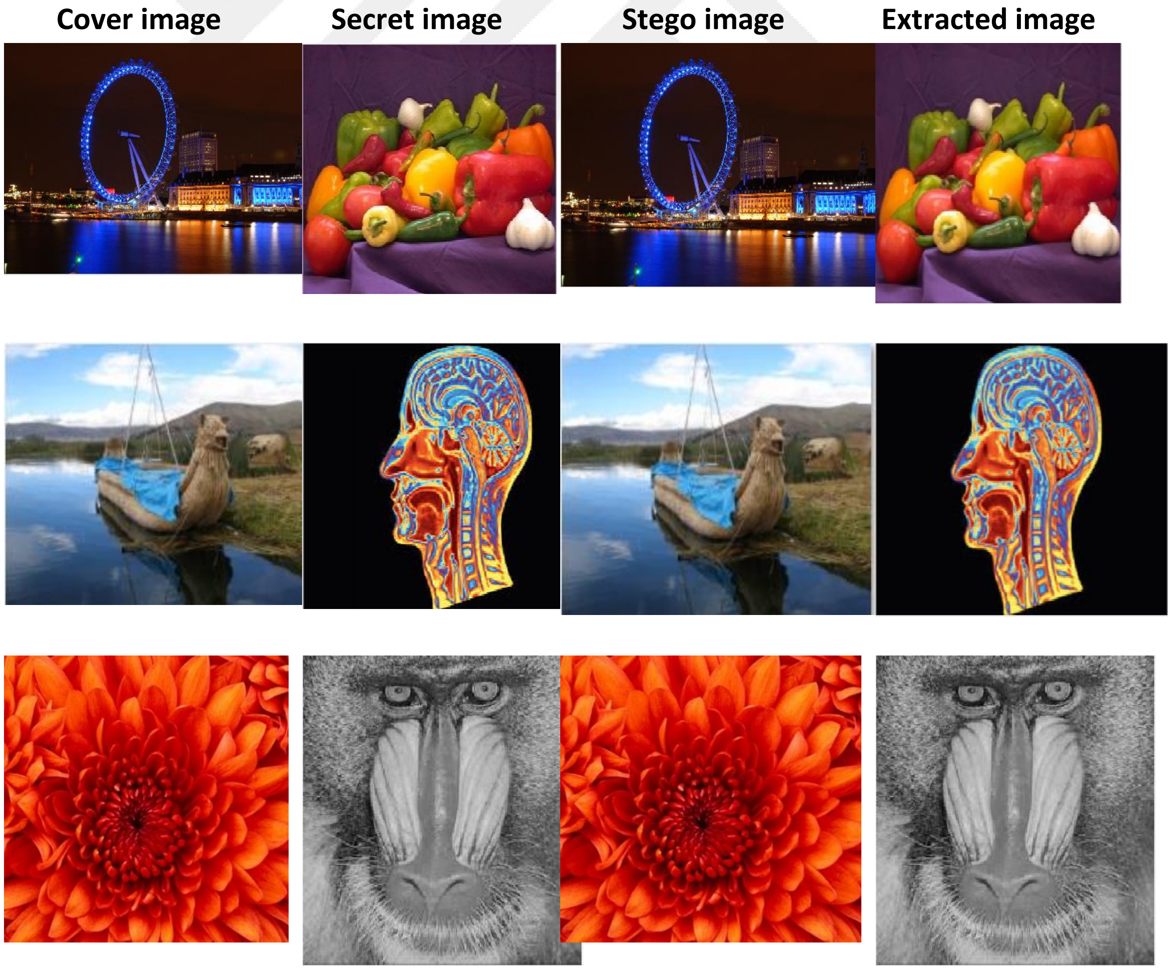


Table 4.13 : Some of results of embedding and extraction processes.

Cover image	Secret image	PSNR Cover vs stego	Cover entropy	secret entropy after qtree	PSNR original secret image vs extracted image	Compression Ratio CR of secret image	Correlation of stego image	Quadtree -th	alpha
London-Eye-night.jpg	Pepper1.jpg	58.3258	6.593	6.0746	38.0817	0.578	0.9999	0.02	0.006
Reed_Islands_of_Lake_Titicaca_-b.jpg	images.jpg	55.8556	7.6695	1.4997	31.1142	1.0362	1.0000	0.0500	0.0090
Chrysanthemum.jpg	babbon. jpg	43.1972	6.1677	7.1819	35.444	0.48	0.9970	0.0100	0.0070

4.8 Comparative Analysis

A PSNR measure is used to test how the stego has been changed through the process of embedding and also for how much the extracted image has been differed from the one originally used.

Two secret images has been used in this comparison to be able to compare between the results obtained from other papers and our work. The below shows the PSNR, MSE ,SSIM and COR for our proposed method and five different methods .The results show that our method proved its effectiveness compare with the methods that have been compared with it.

4.8.1 PSNR of the compare methods for stego image.

Comparison PSNR among the proposed method and (LBS, DWS, M-DWT)[21]. The results showed that the proposed method proved its effectiveness. The table (4.14) shows the results for PSRN for stego image after embedding cameraman as secret image, and. The table (4.15) shows the results for PSRN for stego image after embedding baboon as secret image.

Table 4.14 : PSNR of stego images after embedding cameraman as secret image.

Cover image	**Secret image**	**Proposed method**	**LSB**	**DWS**	**M-DWT**
barbara	cameraman.jpg	**47.0351**	17.67	33.71	44.25
Bird	cameraman.jpg	**53.6064**	12.91	32.37	45.12
Raman	cameraman.jpg	**46.6615**	12.91	32.37	45.23
GoldHill	cameraman.jpg	**44.45402**	11.16	31.86	43.22

Table 4.15 : PSNR of stego images after embedding baboon as secret image.

Cover image	Secret image	Proposed method	LSB	DWS	M-DWT
barbara	baboon.jpg	**46.3381**	13.52	33.15	44.84
Bird	baboon.jpg	**60.5120**	12.91	31.57	43.60
Raman	baboon.jpg	**53.6198**	12.91	31.92	43.36
GoldHill	baboon.jpg	**43.3376**	11.16	32.89	44.98

4.8.2 SSIM among the compared methods for stego image.

In the table (4.16) shows our proposed method is the highest structural similarity index among the compared methods.

Table 4.16 : SSIM comparison among four methods.

Cover image	Secret image	Proposed method	LSB	DWS	M-DWT
barbara	cameraman.jpg	**1**	0.6226	0.8156	0.9725
Bird	cameraman.jpg	**1**	0.6155	0.7941	0.9825
Raman	cameraman.jpg	**0.9998**	0.6279	0.8138	0.9871
GoldHill	cameraman.jpg	**1**	0.6289	0.7887	0.9754
barbara	baboon.jpg	**1**	0.8677	0.8842	0.9921
Bird	baboon.jpg	**1**	0.8569	0.8746	0.9894
Raman	baboon.jpg	**0.9999**	0.8668	0.8869	0.9857
GoldHill	baboon.jpg	**1**	0.8572	0.8795	0.9896

4.8.3 Correlation with original cover image.

Stego correlation test also after testing shows higher correlation with the original data (cover image). The Table 4.17 shows correlation between cover image and stego.

Table 4.17 : Correlation coefficient of stego image.

Cover image	Secret image	Proposed method	LSB	DWS	M-DWT
barbara	cameraman.jpg	**0.99994**	0.9273	0.8631	0.9488
Bird	cameraman.jpg	**0.99998**	0.7913	0.8669	0.9677
Raman	cameraman.jpg	**0.99996**	0.6753	0.8599	0.9378
GoldHill	cameraman.jpg	**0.99987**	0.7069	0.8595	0.9983
barbara	baboon.jpg	**0.99993**	0.7715	0.8423	0.9769
Bird	baboon.jpg	**0.99999**	0.7908	0.8476	0.9917
Raman	baboon.jpg	**0.99999**	0.7668	0.8369	0.9652
GoldHill	baboon.jpg	**0.99985**	0.7527	0.8259	0.9981

4.8.4 Correlation with original secret image

Extracted images correlation test, also after testing shows higher correlation with the original data (secret image). The table (4.18) shows correlation coefficient of extracted cameraman as secret image and the table(4.19) correlation coefficient of extracted baboon as secret image

Table 4.18 : Correlation coefficient of extracted cameraman as secret image.

Cover image	Secret image	Proposed method	LSB	DWS	M-DWT
barbara	cameraman.jpg	**0.9778**	0.9025	0.9187	0.9425
Bird	cameraman.jpg	**0.9965**	0.9422	0.9479	0.9527
Raman	cameraman.jpg	**0.9965**	0.9298	0.9452	0.9576
GoldHill	cameraman.jpg	**0.9780**	0.9594	0.9523	0.9718

Table 4.19 : Correlation coefficient of extracted baboon as secret image.

Cover image	Secret image	Proposed method	LSB	DWS	M-DWT
barbara	baboon.jpg	**0.9538**	0.7945	0.8059	0.8405
Bird	baboon.jpg	**0.9530**	0.7988	0.8008	0.8270
Raman	baboon.jpg	**0.9528**	0.7988	0.8175	0.8364
GoldHill	baboon.jpg	**0.9538**	0.7845	0.7900	0.8268

4.8.5 The fourth method of comparison with our proposed method.

Comparison PSNR and RMSE between the proposed method and 'Image Steganography Scheme using Chaos and Fractals with the Wavelet Transform'[17] method. The results showed that the proposed method was better than the method that was compared with it. The table (4.20) shows the results for PSRN and RMSE.

Table 4.20 : The results for PSRN and RMSE cameraman as a secret image.

	PSNR		RMSE	
Cover image	Chaos-fractal	Proposed method	Chaos-fractal-wavelet	Proposed method
Leaf	35.8950	**40.10678**	4.0906	**2.5188**
Feather	38.2453	**39.98967**	3.1209	**2.5530**
Fragment	37.4657	**44.41132**	3.4139	**1.5345**
Storm	35.5896	**43.35502**	4.2370	**1.7329**

4.8.6 The fifth method of comparison with our proposed method

Comparison PSNR between the proposed method and ‘A DCT-domain System for Hiding Fractal Compressed Images’[15] method. The results showed that the proposed method was better than the method that was compared with it. The table (4.21) shows the results for PSNR.

Table 4.21 : The results for PSNR of stego images.

Cover image	Secret image	**Proposed**	DCT-domain-
		method	Fractal
baboon	baboon	**54.1342**	34.72
baboon	peppers	**54.0538**	37.50
airplane	baboon	**47.6542**	33.19
airplane	peppers	**44.589**	35.42

4.8.7 Wavelet filters

Two types of filters have been used to embed and extract images. Filter used shows no effect on the images extracted. Though some other filters failed either to embed or extract. The table (4.22) shows obtained PSNR in comparison with the Modified DWT and the table (4.23) shows SSIM for stego for two filters, the results demonstrate that proposed method give high PSNR and SSIM.

Table 4.22 : PSNR for Stego for two filters.

Cover	**Secret**	**Haar**	**Sym2**	**Haar**	**Sym2**
image	**image**	**Proposed**	**Proposed**	**M-DWT**	**M-DWT**
		method	**method**		
Bird	cameraman.jpg	**53.6064**	**52.1075**	45.12	47.23
Raman	cameraman.jpg	**46.6615**	**54.4888**	45.23	47.35
GoldHill	cameraman.jpg	**44.45402**	**44.454**	43.22	44.17
Barbara	cameraman.jpg	**47.0351**	**46.4031**	44.25	46.99

Table 4.23 : SSIM for stego for two filters.

Cover	**Secret**	**Haar**	**Sym2**	**Haar**	**Sym2**
		Proposed	**Proposed**	**M-DWT**	**M-DWT)**
		method	**method)**		
barbara	cameraman.jpg	**1**	**1**	0.9725	0.9786
Bird	cameraman.jpg	**1**	**1**	0.9825	0.9841
Raman	cameraman.jpg	**0.9998**	**1**	0.9871	0.9879
GoldHill	cameraman.jpg	**1**	**1**	0.9754	0.9783

4.9 Robustness Test

The art of hiding secret information inside an innocent cover image has two application watermarking and steganography. The first one mostly the information is visible and it is used to incorporate and integrate the information with image fabric, in a way it cannot be removed without destroying the image itself. This has applications in ownership of the image for example. While steganography is to hide information in a way they are not visible. Algorithms of steganography tend to make the hidden information undetectable. Hence every method has its own methods of blocking and detection.

A watermarking system's primary aim is to perform a high level of robustness-that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, however, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it.

Thus there are two types of attacks are available:

1. Deprivation attack: the attacker tries to destroy the information hidden inside the image examples of such attacks rotation at random angles other than special angles, resizing down or up, cropping etc.
2. Detection: the attacker tries to analyze the target image to detect if there are suspicion parts (contains a secret message). Example of this method is the distribution of LSB of cover image, histogram analysis etc.

Always there is a compromise among the targets of watermarking and steganography. Capacity, security, and robustness are the three targets in a triangle of balance when any two is sought to maximize the third is minimized Figure 4.4 shows the explained meaning. In another word Steganography algorithms usually do not require to supply high security against removing or modification of the information message while Watermarking methods require being very robust to try to remove or modify a secret message [16,54]. In our algorithm, we have achieved this balance between the requirements of hiding information that are high security with capacity and acceptable robustness.

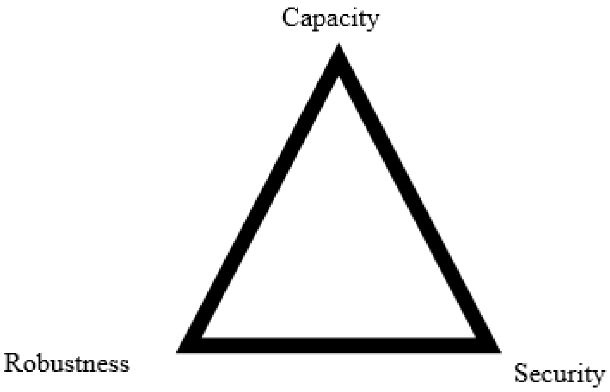


Figure 4.4 : Capacity, security and robustness relation in a hiding system.

4.9.1 Summary of attack results

Table 4.24 shows some of attacks results

Table 4.24 : Summary of attack results.

Method	**Procedure**	**Algorithm Success/failure**
Geometrical	Rotation 30,90,180,270	Success
	Flipping Up down, Left right	Success
	Resizing Up, down	Failure
Detection using statistical methods	BSM (detecting LSB)	Success
	Histogram matching	Matched mostly
	Histogram of the difference image	Small to very small differences

4.9.2 Discussion of attack results

Several histogram matching between stego and original cover images shows a small difference. The difference image histogram also shows slight differences. BSM detection method also fails to detect any randomness in the least bit showing how the least bit distribution is so near the original cover image. Hence, the stego is hardly detected and also a complex method of extraction makes the hidden image secure enough. The algorithm holds for several other attacks like geometrical attacks and shows less resistance to image processing attacks while offering a high capacity of image embedding. Considering this compromise, the algorithm gives decent results in resisting detection attacks. Security and capacity allow large information to be transmitted safely using the proposed algorithm.

4.9.3 Detection application examples

4.9.3.1 Image histogram comparison

A visual inspection of the histogram of stego image and the cover image obtained using the test tool to find differences visually indicating if there is something hidden Figure 4.5 shows the histogram of stego image and cover image. Histogram test shows if there are any changes in the frequency of image color pixels.

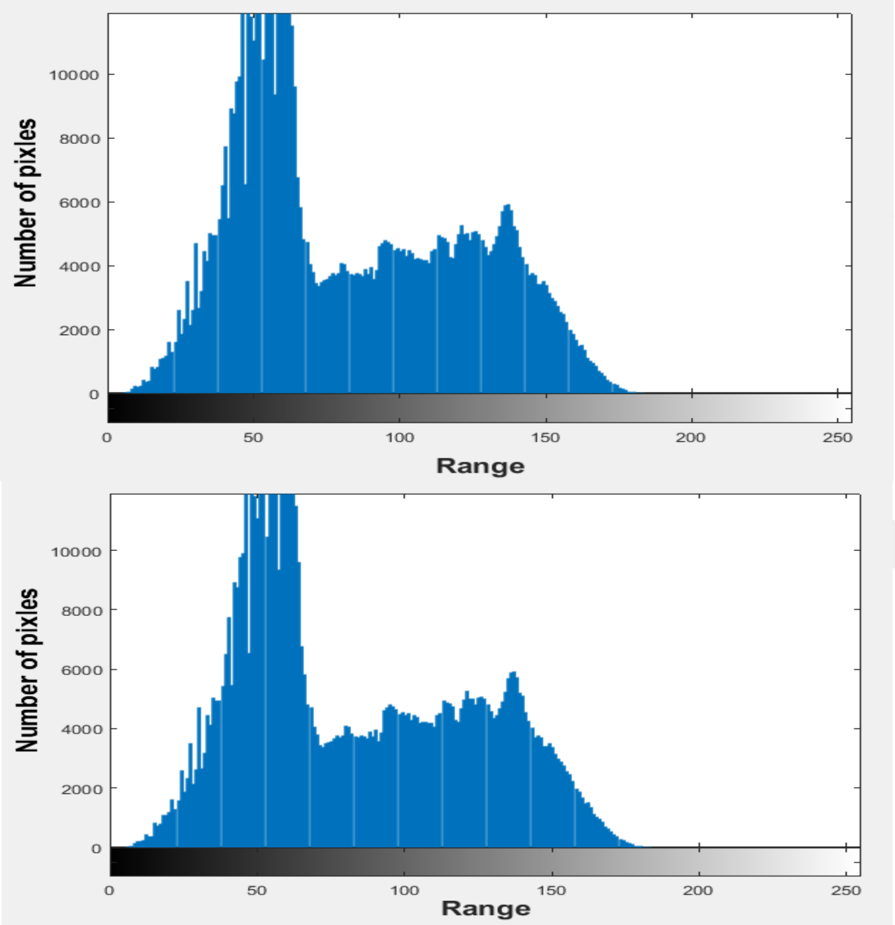
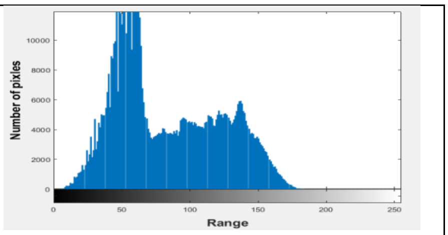
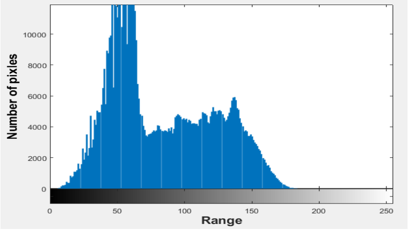
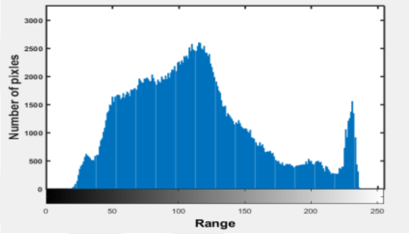
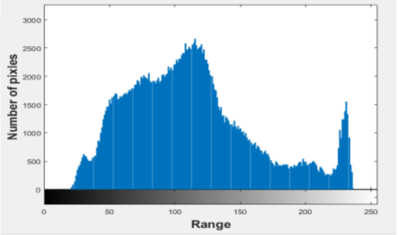
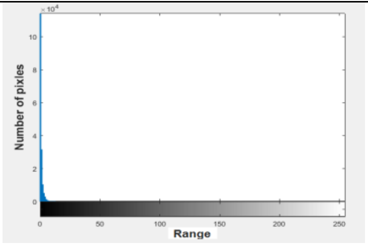
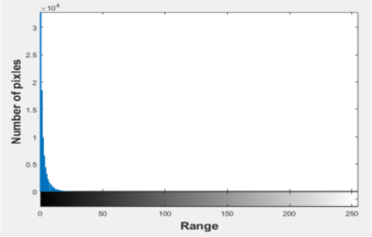


Figure 4.5 : Cover and stego images histogram.

4.9.3.2 Image difference histogram

histogram of Stego and cover image are subtracted from each other, then the histogram is built from the difference. If the two images are identical either no histogram appear or slightly difference histogram is shown Table 4.25.

Table 4.25 : Histogram of the image difference.

 Cover image	
 Stego image	
 Cover image	
 Stego image	
 Flower histogram of the difference	 Gold hill histogram of the difference

4.9.3.3 BSM detection method

The least bit is inspected for hidden information where every bit is extracted from the suspected stego and rebuilt as a black and white image revealing the distribution of the bits whether they reflect the same original stego suspected image or them are merely a random noise is they were random then there is a high chance that the tested image is a stego [55] (cf. Figure 4.6).

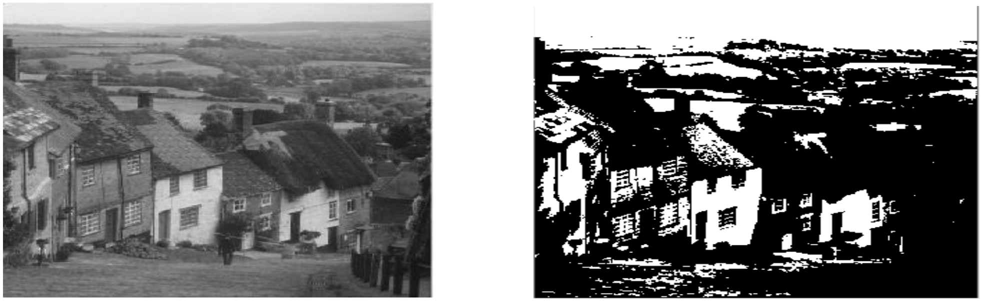


Figure 4.6 : Example of BSM method.

the table 4.26 show comparison our proposal with other methods by using Image processing attacks, the results were acceptable.

Table 4.26 : PSNR of stego image after attacks, cameraman as Secret Image.

Stego image	**Methods**	**Rotation**	**Sharpening**	**Gamma correction**
Barbara	**Proposed**	**30.6292**	**35.8431**	**39.4743**
	LSB	10.86	10.21	10.67
	DWS	16.90	21.58	16.08
	M-DWT	40.85	38.08	16.08
Bird	**Proposed**	**35.550**	**36.1123**	**39.7885**
	LSB	11.27	11.16	10.87
	DWS	28.91	26.42	18.32
	M-DWT	37.01	34.34	31.63
Raman	**Proposed**	**31.5274**	**24 .03**	**39.7354**
	LSB	10.37	10.09	10.64
	DWS	12.75	21.88	11.05
	M-DWT	38.23	35.82	34.87
Gold Hill	**Proposed**	**30.008**	**38.4103**	**38.4103**
	LSB	10.93	10.71	10.05
	DWS	21.31	11.23	21.91
	M-DWT	37.37	27.65	32.31

4.9.4 Adding spots to stego image and try to extract the secret image

Table 4.27 shows results of adding a dark spot on the stego image and chances to restore the secret image. At different spot sizes with randomly located of the stego image to study success/failure rate depending on the size and location of the spot.

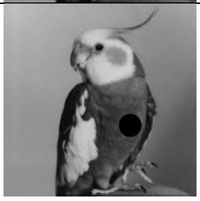
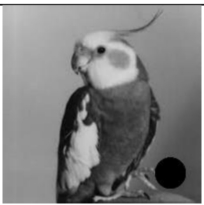
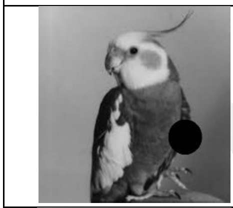
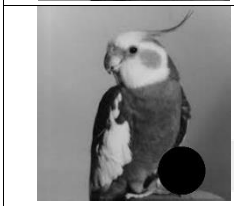
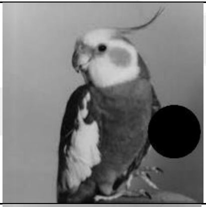
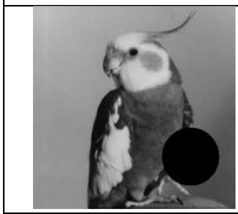
The chances are high to extract successfully. The fact that the secret is hidden not in a sequence of locations decrease the possibility to destroy the information hidden also the nature of wavelet decomposition as it deals with abrupt changes in the image also participate in decreasing the effect of the spots noise. Thus the extraction is possible in spite of the noise that is presented.Table 4.28 shows stego image after adding spots with randomly located.

Table 4.27 : Success/failure rate to extract the secret image after adding spots with randomly located.

Spot size(pixels)	Success
10	yes
30	yes
40	yes
60	yes
80	yes
90	yes
100	yes
125	yes
135	yes
145	yes
155	No

Generally, attacks can be resisted and reversed thus retaining the stego and extraction is a success. This is realized through detection and geometrical attacks(rotation, flipping etc.) while image processing attacks show a considerable amount of success rate. Gamma correction can be retained using different screen properties since they are changing from 1.8 – 2.2 it is not difficult to set a special correction value which can reestablish the original stego. This factor also can be overcame using gamma correction before embedding, thus depriving the attacker of using this attack effectively. Sharpening attack made also a good rate of success since it can be reversed by applying the reverse filter. Using attacks and leaving effect is considered when a noticeable change is made over the abrupt changes in the colors of the image which affects wavelet transform. The latter leads to an inability to find the secret vector location and no extraction is possible. Considering adding noise to the image is inspected using a changed size of a spot added to the image which shows high success rate even when the spot size is considerably large. The presentation of spot affects part of the image randomly selected shows lower PSNR as the spot gets larger yet the secret can be extracted.

Table 4.28 : Stego image after adding spots with randomly located.

Stego image after adding spot	pixels number of the spot diameter	Stego image after adding spot	pixels number of the spot diameter
	10		30
	60		80
	90		100
	125		135
	145		155

4.10 The Relationship Among Size of Secret İmage, Compression Ratio and PSNR of Stego

Table 4.28 shows the relationship of resizing the secret image with using the same image as the cover image, we used cameraman image as a secret image and the bird image as a cover image. The result appeared that PSNR of stego image decreases when the size of the secret image increase. The Figure 4.7 this relationship clarifies.

The figure 4.9 shows the relationship of resizing the secret image with using the same image as the cover image. The result appeared that compression ratio of the secret image decreases when the size of the secret image decrease.

Table 4.29 : The relationship among size of secret image, compression ratio and PSNR of stego.

Secret Image Size(pixels)	Secret Image Compression Ratio	Quad Tree Threshold	Stego PSNR
64	1.1359	0.05	60.2624
128	1.5171	0.05	60.2169
256	1.839	0.05	58.7491
512	3.4391	0.1	47.8104

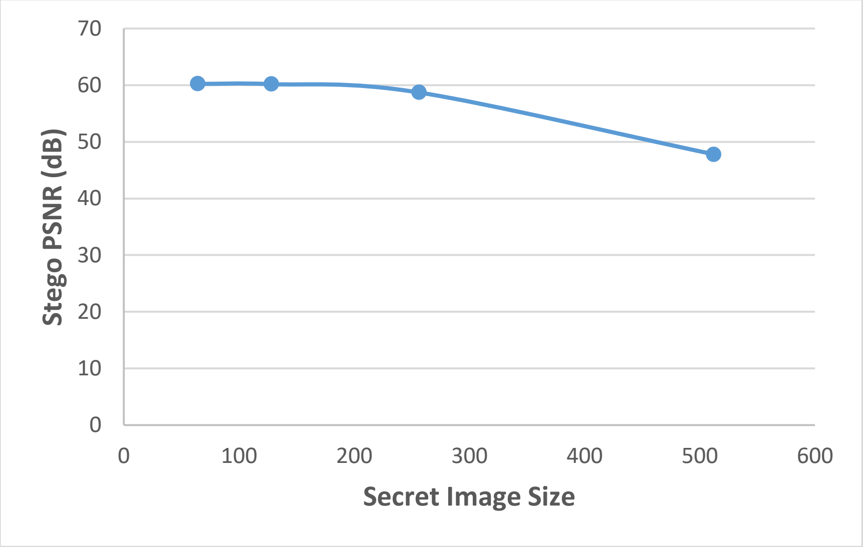


Figure 4.7 : The relationship between secret image size and PSNR of stego image.

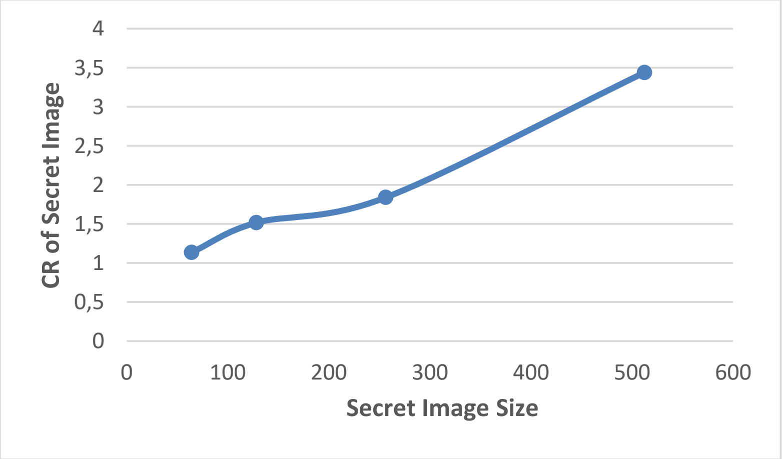


Figure 4.8 : The relationship between secret image size and compression ratio.

The table4.30 shows the effect of change in the size of spots on PSNR of the stego image.

Table 4.30 : The change of stego image with the change of spots.

Diameter Size (pixels)	Spot Size (pixels)	PSNR of Stego image
1	4	51.8673
3	12	46.8983
6	37	47.1633
10	97	37.2543

4.11 Discussion

4.11.1 Fractal as a compression tool

A high compression ratio is achieved using fractal and Huffman encoding. While high and efficient compression is proven using fractals, the use of hybrid method of a fractal and Huffman gives more compression ratio. Steganography demands of high compression to make secret vector as small as possible. Figure 4.6 shows compression ratio going up as the threshold is higher, but the latter affects the output image causing some distortion. the red curve shows how the block size affects compression producing very high compression ratio and also producing distortions at the high levels.

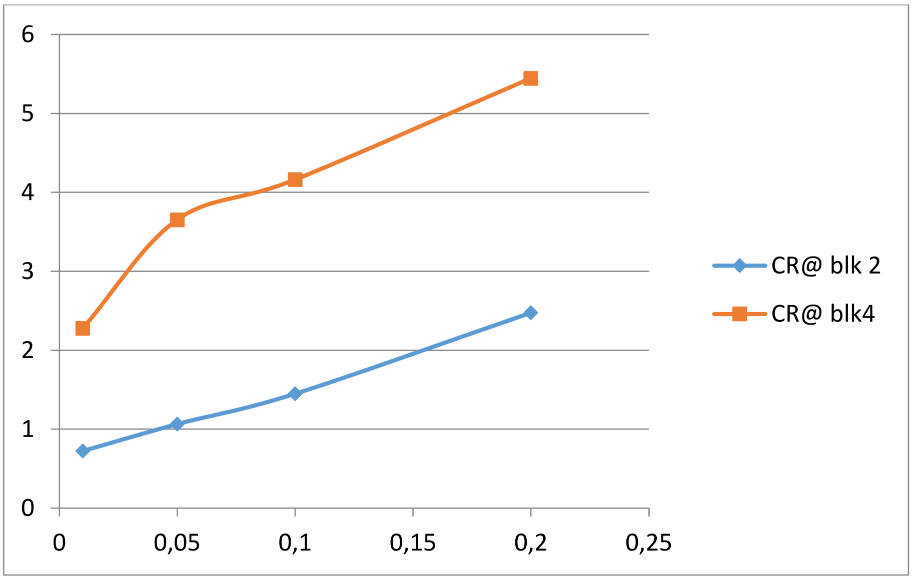


Figure 4.9 : PSNR vs QuadTree Threshold value for cameraman with min block 2×2 and with min block 4×4.

The distortion can be compensated using filters. Nevertheless, the worst case the image is still recognizable. thus it can be used to dramatically generating high compression.

4.11.2 Using wavelet to hide information

The storage of secret information in high frequency components of a digital image after decomposition using wavelet makes the identification by human eye very difficult. The use of such technique allows for getting a large number of insignificant coefficients which they allow as possible an amount of secret information to be embedded without deteriorating the cover to the sensed degree.

4.11.3 Mapping secret using thresholding

Using a certain threshold value calculated during the embedding time adds difficulty to extract secret information inside an image. The threshold is calculated by the standard deviation of coefficients value, that proved more effective in producing more locations than using the average. Another image can not produce the same map. The map is from a side depending on the cover and from another side depend on the secret. It is not easy to determine the correct mapping that makes more security.

4.11.4 Complexity of the hybrid method

Converting using Quad tree, encoding, transforming, finding a threshold value and hiding makes it very difficult to extract such information rather destroyed than extracted correctly.

Generating the map depending on twice converted (fractal and Huffman) for secret information that makes it very difficult to detect and to extract the secret image.

5. CONCLUSIONS AND RECOMMENDATIONS

Hide confidential data in order to preserve them from any external influences. Therefore, the secret image is hidden inside another image as a cover, to hide the data with condition there is no obvious change in the form of cover image, and not knowing that there are data hidden, so as not to be extracted. Also we did not add any additional data to work on the protection of privacy data.

There are many different algorithm and embedding methods that enable us to hide information a given object. However, all of the algorithms and techniques should satisfy certain requirements so that steganography can be applied correctly. The following is a list of main requirements that steganography techniques must satisfy:

1. The integrity of the secret image after it has been embedded inside the cover image the output (stego image) must be correct.
2. The secret message They should not be manipulated in any way, like additional information being added, loss of information or changes to the secret image after it has been hidden.
3. If secret image is altered over steganography, it would defeat the whole point of the process.
4. The stego image must stay unaltered or almost unaltered to the naked eye. If the stego image alters important and can be observed, a third party may see that information is being hidden and, so could try to extract or to destroy it.

In this thesis, we used the Wavelet transform, which gave good compression of cover image. Also we used fractal image decomposition and Huffman code of secret image to make it more security (double compression is powerful to allow more secret volume to be hidden).

The threshold was utilized as a strategy to decide the concealing guide and to extraction. the compression is concerning with entropy. The outcome of extracted images was high resolution. This algorithm was used in the field of information security and privacy, and the results demonstrate its effectiveness, robustness and safe method to save privacy.

The future work may be listed as follows:

1. Developing fractal function to accommodate a higher accuracy value and more data.
2. Further development to hidden vector by converting it to frequency domain before embedding it to wavelet.
3. Coding color images with a single Huffman dictionary in order to shorten the length of information to hide.

REFERENCES

[1] **Pommer, A. (**2003). *Selective Encryption of Wavelet –Compressed Visual Data*, Ph.D. Thesis, submitted to Salzburg university.

[2] **Seo, Y, Kim, D, Yoo, J, Dey, S, and Agrawa, A.** (2003). Wavelet Domain Image Encryption by Subband Selection and Data Bit Selection, *Proceeding of the world wireless conference*, USA, pp.50-55.

[3] **Al-Dilaimy, U, I.** (2001). *Text in image Steganography*, M.Sc. Thesis, Electrical Engineering Department University of Technology.

[4] **Boukhonine, S.** (2002). Cryptography: A Security Tool of the Information Age , Garener Group Research Note, pp.1-17.

[5] **Na-l Wa. (**2004**)**. *A Study on Data Hiding Gary Level and Binary Image* , A Ph.D. Thesis submitted to Chaoyaug University of technology.

[6] **Neil, Johnson, and Jojodia.** (1998). Exploring Steganography Seeing The Unsee ,*IEEE Computer*, Vol,31, No. 2, pp.26-34.

[7] **Katzenbeissers, S, and Petitcolas, F, A.** (2000). Information Hiding Technique for Steganography and Digital Watermarking, Arteck House, London.

[8] **Richer, p.** (2002). Steganalysis: Detection Hidden Information with Computer A-nalysis, Proceeding of SPIE Conference on Data Mining, pp.11-15.

[9] **Jadhav, S. , and Rawate, A.** (2016). A New Audio Stega- nography with Enhanced Security based on Location Selection Scheme, *IJE SC*.

[10] **Steganography and Digital Watermarking**.*https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.htm*.date retrieved 15.08.2017.

[11] **Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., Baik, S. W.** (2015). A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption. TIIS, 9(5), 1938-1962.

[12] **Yadav, D., Kaur, J. (**2016**)**. Conceal and Secure Communica- tion System, Volume 6, Issue 6.

[13] **Doshi, R., Jain, P., Gupta, L.** (2012). Steganography and Its Applications in Security, Vol.2, Issue.6. pp.4634-4638.

[14] **Sonika C. Rathi, V. S. Inamdar,** (2012). Medical images authentication through watermarking preserving ROI. *Health Informatics-An International Journal (HIIJ), 1(1).*

[15] **Chang, C., Chiang, C., and Hsiao, J.** (2005). A DCT-domain system for hiding fractal compressed images. In IEEE *Advanced Information Networking and Applications*, 2005. AINA 2005. 19th International Conference on (Vol. 2, pp. 83-86).

[16] **Al-Ataby and Al-Naima.** (2010).A Modified High Capacity Image Steganography Technique Based on Wavelet Transform, *The International Arab Journal of Information Technology*, Vol. 7, No. 4.

[17] **Wu,Y. and Noonan, J.** (2012). Image Steganography Scheme using Chaos and Fractals with the Wavelet Transform, *Int. J. Innov. Manag. Technol*, Vol. 3, no. 3, pp. 285–289.

[18**] Prabakaran, G., Bhavani, R., and Rajeswari,P.** (2013). Multi secure and robustness for medical image based steganography scheme. *In Circuits, Power and Computing Technologies (ICCPCT)*, 2013 International Conference on (pp. 1188-1193). IEEE.

[19] **Abbas, T., Hamza, H.** (2014). Steganograp- hy using Fractal Images Techniqu- e. *IOSR Journal of Engineering*,4, 52-61.

[20] **Pal Samir, S.** (2016). Image Steganography using Block Level Entropy Thresholding Technique, *J. Res.*, vol. 2, no. 4, pp. 9–11.

[21] **Kumar,V and Kumar,D.** (2017). A modified DWT-based image steganography technique. Multimedia Tools and Applications, 1-30.

[22] **Fridrich, M. and Goljan, D.** (2004). Searching for the Stego Key, (PDF). Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. 5306: 70–82.

[23] **Krenn, R.** (2003). Steganography and Steganalysis, *http:www.krnn.nl/univ/cry /stegl.*

[24] **Krenn, J.** (2004). Steganography and Steganalysis, *https://pdfs. Semanticscholar.org/62cf/e5d45490202f6136a914555ba654808b0d96.pdf.*

[25] **Abbas C., Joan C., Kevin C. and Paul M.**. (2010). Digital Image Steganography: Survey and Analysis of Current Methods, *Signal Processing*, Volume 90, Issue 3.

[26] **The Types and Techniques of Steganography Computer Science Essay**.*https :// www.ukessays.com/essays/computer-science/the-types-and-techniqu es-of -steganography-computer-science-essay.php,*date retrieved 07.03.2017.

[27] **Steganography and Digital Watermarking**. *https://www.cs.bham.ac.uk/~mdr/ teaching/modules03/security/students/SS5/Steganography.htm*,date retrieved 07.06.2017.

[28] **Babatunde, S. (**2012). Discrete wavelet mathematical transformati- on method for non-stationary heart sounds signal analysis, *ARPN Journal of Engineering and Applied Sciences,* vol. 7, no. 8. pp.1021-1028.

[29] **Robi, P.** The Wavelet Tutorial, *http://user.rowan.edu /~polikar /WAVEL ETS/WTpart1.html*, Fundamental Concepts & an Overview of the Wavelet T -heory. The Wavelet Tutorial is hosted by Rowan University, College of Engineering Web Servers, (Last accessed on Dec. 27th, 2017).

[30] **Shaamala, A., Abdullah, S. M., and Manaf, A. A.** (2011). The Effect of DCT and DWT Domains on the Robustness of Genetic Watermarking. Informatics Engineering and Information Science, pp.310-318.

[31] **Charles, K.** (1992). An Introduction to Wavelets, Academic Press, San Diego, ISBN 0-585-47090-1.

[32] **Anthony D Angelo.** (2016) A Brief Introduction to Quad trees and Their Applications, Style file from the 28th Canadian Conference on Computational Geometry.

[33] **Veenadevi,S.V and Anant, A.G.**(2012). Fractal image compression using quad tree decomposition and huffman coding. Signal & Image Processing, 3(2),2 07.

[34] **Milan, S., Vaclav, H. and Roger, B.** (2014). Sonka, M., Hlavac, V., & Boyle, R. (2014). Image processing, analysis, and machine vision. Cengage Learning. pp. 108-109.

[35] **Addison,P.S. (**1997). Fractals and chaos: an illustrated course. CRC Press.

[36**] Huffman and D.** (1952). A Method for the Construction of Minimum-Redundancy Codes, (PDF). Proceedings of the IRE. 40 (9): 1098–1101.doi:10.1109/J RPROC.1952.273898.

[37] **Van Leeuwen**, J. On the construction of Huffman trees, in: Proceedings Third International Colloquium on Automata, Languages and Programming (ICALP), 1976, 382–410.

[38] **Huffman code binaryyessence.** *.http://www.binaryessence.com/dct/en000079. Htm,* date retrieved 22.06.2017.

[39] **Utpal, N. and Jyotsna, K.** (2014). Fractal image compression by using loss-less encoding on the parameters of affine transforms. In Automation, Control, Energy and Systems (ACES), 2014 First International Conference on (pp. 1-6). IEEE.

[40] **Root Mean Square Eerror.** (2012). *http:// www.kaggle .com/wiki /Meterics/history/,* date retrieved 03.06.2017.

[41] **Wang, Z., Simoncelli, E.P. and Bovik, A.C.** (2004).Multiscale structural similarity for image quality assessment, *Conference Record of the Thirty-Seventh Asilomar Conference on Signals, Systems and Computers*, **2**: 1398–1402 Vo l.2.

[42] **Tarik Z. and Hanoon,A.** (2012). Design & evolution of a steganography systeem for speech signal by slantlet transform,Vol. 05, No. 02, pp. 9 9-113,

[43] **Starosolski, R.** (2007). Simple fast and adaptive lossless image compression algorithm, Softw. - Pract. Exp., vol. 37, no. 1, pp. 65–91.

[44] **Lin, P.** (2009). Basic Image Compression Algorithm and Introduction to JPEG Standard, no. Mv, pp. 1–15.

[45] **Wu,Y and Noonan, J.** (2012). Image Steganography Scheme using Chaos and Fractals with the Wavelet Transform, *Int. J. Innov. Manag. Technol.*, vol. 3, no. 3, pp. 285–289.

[46] **Shannon, Claude E.** (1948). A Mathematical Theory of Communication, *Bel System Technical Journal*. 27 .

[47] **Henry Lee, T.** Wavelet Analysis for Image Processing, Institute of Communication Engineering, National Taiwan University, Taipei, Taiwan,RO-retrieved 11.07.2017.

[48] **Gonzalez, R and Woods, R. E**. (1992). Digital image processing, 4th edition, Addison-wesley Reading..

[49] **Milan S., Vaclav, H., and Roger, B.** (2014). Image Processing An- alysis and Machine Vision. *https://books.google.com/books?id=DcETCgAA QBAJ). p. 108-109*.

[50] **Fischer, Yuval .**(1992). Przemyslaw Prusinkiewicz, ed. SIGGRAPH'92 course notes - Fractal Image Compression. SIGGRAPH *.http://www.siggraph.org/. Fractals -From Folk Art to Hyperreality. ACM SIGGRAPH.*

[51] **Kekre, H., Tanuja K., and Sanjay, R .** (2011). Image reconstru- ction using Fast Inverse Halftone & Huffman coding Technique, *IJCA*, vol- ume 27-No 6, pp.34-40.

[52] **Data compression ratio.** (2013)*https://en.wikipedia.org/wiki/Datacompression ratio,* date retrieved 12.10.2017.

[53] **Coding Theory.** *http://www.cs.unm.edu/~storm/cs530/Coding.htm*,date retrieved 29.06.2017.

[54] **Eugene T. Lin and Edward J. Del. (**1999). A Review of Data Hiding in Digit al Images, *IS&T's PICS Conference*.

[55] **Mehdi, K., Husrev, T., and Sencarb, N.** (2005). Benchmarking steganographic and steganalysis techniques, Polytechnic University, Brooklyn , NY 11201, USA.

CURRICULUM VITAE

Name Surname : Suhad ALBASRAWI

Place and Date of Birth : Iraq/Baghdad 8/1/1972

E-Mail : suhad7242@gmail.com

EDUCATION **B.Sc :** 1996, AL-Mustansiriyah University, Education , Computer Science Department.